VAP Outdoor Access Point

User's Manual

Copyright

Copyright © 2012 all rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the supplier.

About This Manual

This user manual is intended to guide professional installer to install the VAP Access Point and how to build the infrastructure centred on it. It includes procedures to assist you in avoiding unforeseen problems.

Conventions

For your attention on important parts, special characters and patterns are used in this manual:

Note:

- This indicates an important note that you must pay attention to.

Warning:

- This indicates a warning or caution that you have to abide.

Warranty

Hardware warranty is for one (1) year from date of shipment from Distributor warrants that hardware will conform to the current relevant published specifications and will be free from material defects in material and workmanship under normal use and service.

Contents

1. Chapter 1 Introduction 4
   1.1. Introduction 4
   1.2. Key Features 4
   1.3. Hardware Overview 5
   1.4. Typical Management Scenario 7
   1.5. Typical Application Scenario Thin-AP Mode 7
   1.6. Typical Application Scenario AP Mode 7
2. Chapter 2 Hardware Installation 9
   2.1. Preparation before Installation 9
   2.2. Product Package 9
   2.3. Hardware Installation 11
      2.3.1. Connect up 11
      2.3.2. Pole Mounting 20
      2.3.3. Using the External Antenna 21
      2.3.4. Using the Grounding Wire 22
3. Chapter 3 Quick Start Tutorial 23
   3.1. Access the Web Configurator 23
   3.2. Configure the AC+Thin AP mode 25
   3.3. Firmware Upgrade for VAP AP in AC mode 30
   3.4. Install the VAP-Managed AP 30
   3.5. Manage the VAP-managed APs 31
   3.6. Firmware Upgrade for VAP AP in AC mode 32
   3.7. Monitor the VAP-Managed AP 33
   3.8. Configure the Fat AP mode 34
4. Chapter 4 Navigate the Web Configurator 41
   4.1. AC+Thin AP Mode 41
      4.1.1. Status 41
      4.1.2. Wireless Settings 40
      4.1.3. Wireless Protocols 44
      4.1.4. Access Control 47
      4.1.5. Traffic Shaping 48
      4.1.6. Radius Settings 48
      4.1.7. TCP/IP Settings 50
      4.1.8. Captive Portal 50
      4.1.9. Firewall Settings 52
      4.1.10. Management 55
      4.1.11. Tools 63
   4.2. Thin AP Mode 65
      4.2.1. Information 65
      4.2.2. Basic Settings 65
   4.3. FAT AP Mode 66
      4.3.1. Status 66
      4.3.2. System 70
      4.3.3. Wireless 79
      4.3.4. Remote Management 96
      4.3.5. Tools 102
5. Appendix A. ASCII 106
6. Appendix B. SSH Settings 107

1. Chapter 1 Introduction

1.1. *Introduction*

The IEEE 802.11b/g/n VAP Access Point is a multi-mode Access Point embedded with a software-based virtual access controller for centrally managing VAP-managed APs (Thin AP) that eliminates the need for a separate hardware controller to manage the WLAN. By creating a single virtual-WiFi network that encompasses all of the APs in the network users perceive the WiFi as a single wireless connection with a single SSID and security settings. As well as giving centralised AP management the single, virtual AP also eases client roaming between nodes giving practically seamless roaming capability. Ideal for SMB or hotspot network, this breakthrough innovation provides superior Wi-Fi network solutions at significantly lower cost and easier management.

While operating as access point, the VAP Access Point also provides centralized management and monitoring of all the VAP-managed APs on the network. The VAP Access Point is capable of supporting up to 50 VAP-managed APs.

In addition, the easy-to-install VAP Access Point is also a high-performance last-mile broadband solution that provides reliable wireless network coverage for outdoor broadband application.

1.2. *Key Features*

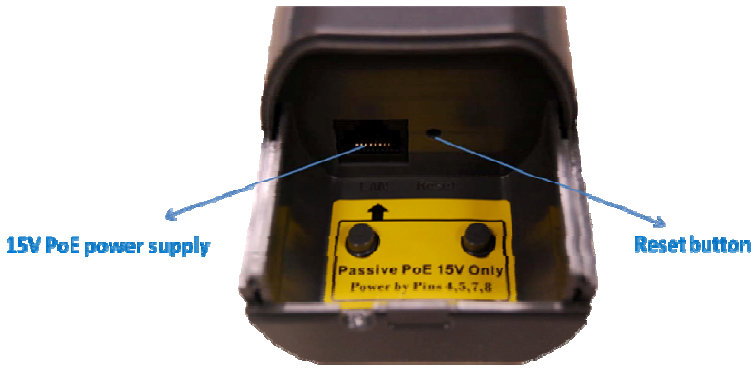
- Centralized configuration control for your network
- Virtual WiFi network configuration (common SSID and WiFi security)
- Client Roaming capabilities
- Compliant with IEEE 802.11n standard
- Support passive PoE supplied with 15V.
- High reliable watertight housing endures almost any harsh environments
- Three management modes including AC+Thin AP, Thin AP and Fat AP.
- Four wireless operation modes including AP, Wireless Client, WDS and AP Repeater.
- Up to 16 BSSIDs available for service deployment
- Support encryption: 64/128/152-bit WEP and 802.1X, WPA, WPA2, WPA&WPA2,WPA-PSK, WPA2-PSK, and WPA-PSK&WPA2-PSK
- User-friendly Web and SNMP-based management interface

1.3. *Hardware Overview*

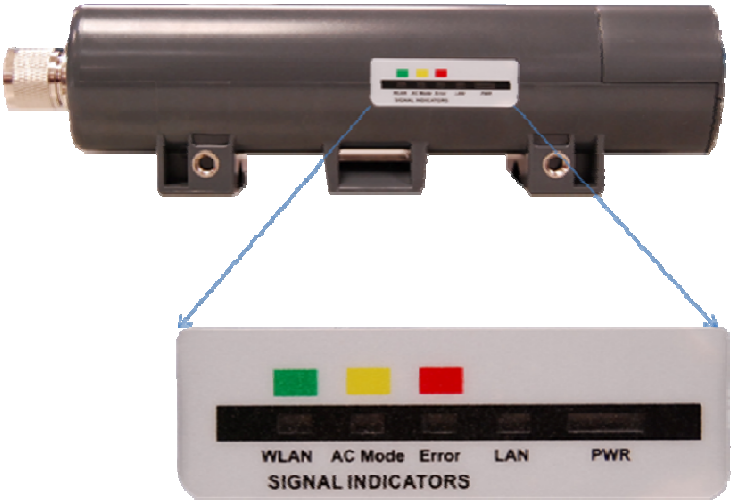
Front View

Back View

Inside the Bottom Cover



Side View



LED Indicators

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The device is powered on
		Off	The device is not receiving power
	Amber	Blinking	The device is in initialization process
LAN	Green	On	The device has the Ethernet connection
		Off	The device has no Ethernet connection
		Blinking	Transmitting/receiving Ethernet packets
WLAN	Green	Off	The WLAN is inactive
		Blinking	Transmitting/receiving wireless packets
AC Mode	Yellow	Off	The device is not in AC mode
		On	The device is in AC mode
Error	Red	Blink 1 time every 2 secs	The Thin AP has not been configured by the AC
		Blink 2 times every 2 secs	The Thin AP has lost connection with the AC

1.4. *Typical Management Scenario*

This section describes the typical management of VAP Access Point. By default, it is set to thin AP mode (VAP-managed AP) which allows it to be managed by the VAP Access Point in AC+Thin AP mode. The VAP Access Point allows the administrator to manage up to 50 VAP-managed APs. So a typical application might consist of a centralised VAP set in AC mode controlling multiple VAP units set in thin AP mode. So, in operation, each VAP Access Point in thin AP mode joins a wired network which gives backbone connectivity (in actual fact the backbone connectivity between the VAP units could take several different forms, for example via a separate WiFi network interconnecting the nodes together). Then it looks for a VAP Access Point in AC mode. If there is a wireless controller on the network, the VAP-managed AP will send the registration request to the VAP Access Point. Once the registration is successfully made, the VAP Access Point will add the VAP-managed AP to its management list and provides it with default configuration information.

1.5. *Typical Application Scenario Thin-AP Mode*

This mode is where you want to use a network of controlled units which merge together to give the appearance, from the clients point of view, of a single WiFi network. Presenting the network as single WiFi simplifies connectivity for the end users and improves roaming for clients between the nodes.

In operation you have one VAP unit which is nominated as the AC controller unit. This is set to mode AC+Thin AP. This is the main management AP which is used to centrally configure and control the other APs. The remote APs are configured in Thin AP mode. All of the remote Thin APs must be connected (via their lan port) to the network port of the AC unit i.e. all the APs must be on the same network. The backbone interconnectivity between the APs can be via a standard copper-based LAN system or, if this is impractical, for example if you are distributing the Thin AP units over a wide site where there is no LAN connection to each AP unit, then you could use a separate WiFi network for the infrastructure e.g. you might have a point-to-multi-point 5GHz WiFi network doing the backbone via 5GHz bridge units connected to each AP and then aimed back at the source. Obviously this means you have two units at each location i.e. the Thin AP unit and also, maybe located on the same fixing pole or possibly located nearby, would be the 5GHz bridge unit.

1.6. *Typical Application Scenario AP Mode*

This section describes the typical applications of VAP Access Point. By default, it is set to AP mode which allows it to establish a wireless coverage; besides, it is also able to join any available wireless network under wireless client mode.

AP
Wi-Fi Coverage
Wireless Client
AP

2. Chapter 2 Hardware Installation

This chapter describes product information you have to know and check before installing the VAP Access Point.

2.1. *Preparation before Installation*

Professional Installation Required

If you do not feel confident to affect the installation then please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.

Installation Precautions

To keep the VAP Access Point well while you are installing it, please read and follow these installation precautions.

1. Users MUST use a proper and well-installed grounding and surge arrestor with the VAP Access Point; otherwise, a random lightening could easily cause fatal damage to VAP Access Point. EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRNTY.
2. Users MUST use the "Power cord & PoE Injector" shipped in the box with the VAP Access Point.
Use of other options will likely cause damage to the unit.
3. Users MUST power off the VAP Access Point first before connecting the external antenna to it. Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external antenna onto the unit; otherwise, damage might be caused to the VAP Access Point itself.

2.2. *Product Package*

The product package you have received should contain the following items. If any of them are not included or damaged, please contact your local vendor for support.

- VAP Access Point t ×1
- Pole Mounting Ring ×1
- Power Cord & PoE Injector ×1
- Grounding Wire Kit ×1
- Product CD ×1

Note:

- Product CD contains Quick Installation Guide and User Manual.

Pole Mounting Ring

Power Cord & PoE Injector

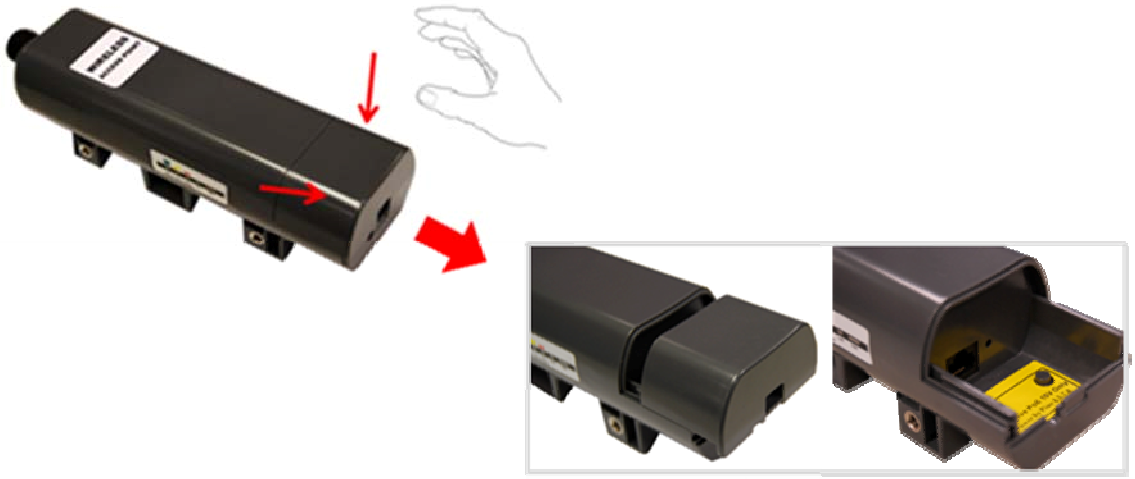
Warning:

- Users MUST use the “Power cord & PoE Injector” shipped in the box with the VAP Access Point. Use of other options will likely cause damage to the unit.

2.3. *Hardware Installation*

2.3.1. Connect up

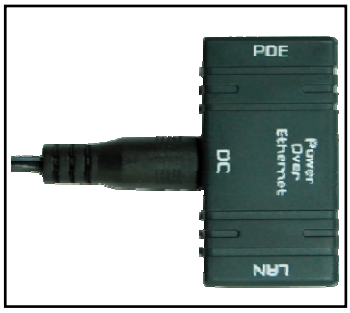
1. The bottom of the VAP Access Point is a movable cover. Grab the cover and pull it back harder to take it out as the figure shown below.



2. Plug a standard Ethernet cable into the RJ45 port.

3. Slide the cover back and press down the lock button to seal the bottom of the VAP Access Point.

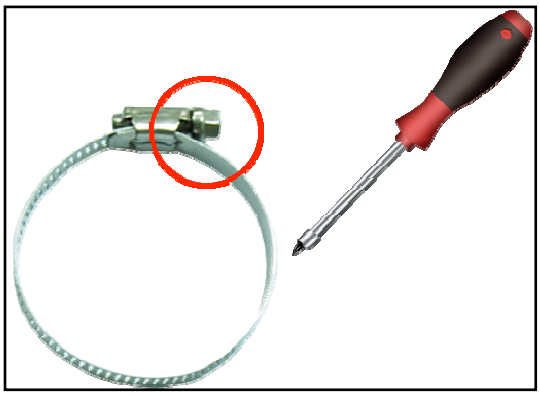
4. Plug the power cord into the DC port of the PoE injector as the following right picture shows.



5. Plug the other side of the Ethernet cable into the “POE” port of the PoE injector and get the complete set ready. Connect the unit to the network with an Ethernet cable connected to the “LAN” port of the PoE injector.

2.3.2. Pole Mounting

1. Turn the VAP Access Point over. Put the pole mounting ring through the middle hole of it. Note that you should unlock the pole mounting ring with a screw driver before putting it through the device as the following right picture shows.

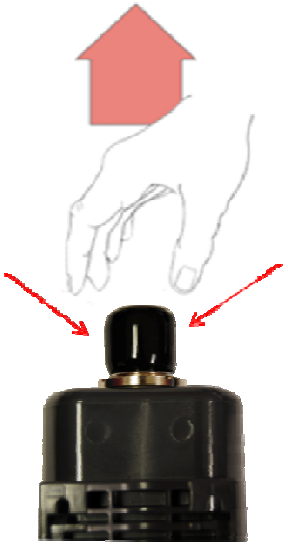


2. Mount the VAP Access Point steadily to the pole by locking the pole mounting ring tightly.

2.3.3. Using the External Antenna

If you prefer to use the external antenna with N-type connector for your application instead of the built-in directional antenna, please follow the steps below.

1. Grab the black rubber on the top of VAP Access Point, and slightly pull it up. The metal N-type connector will appear as shown below.



2. Connect your antenna to the N-type connector on the top of unit.

Note:

- Before using the external antenna with the N-type connector to the VAP Access Point, users should prepare the cable in advance, if needed.
- While connecting the N-type connectors, users should pay attention to the forces they use in prevention of the damage for N-type connectors.

Warning:

- Users MUST power off the VAP Access Point first before connecting the external antenna to it. Do not switch from built-in antenna to the external antenna from WEB management without physically attaching the external antenna onto the unit; otherwise, damage might be caused to the VAP Access Point itself.

2.3.4. Using the Grounding Wire

The VAP Access Point is equipped with a grounding wire. It is important that the wireless bridge, cables, and any supporting structures must be properly connected to earth ground during normal use against surges or ESD.

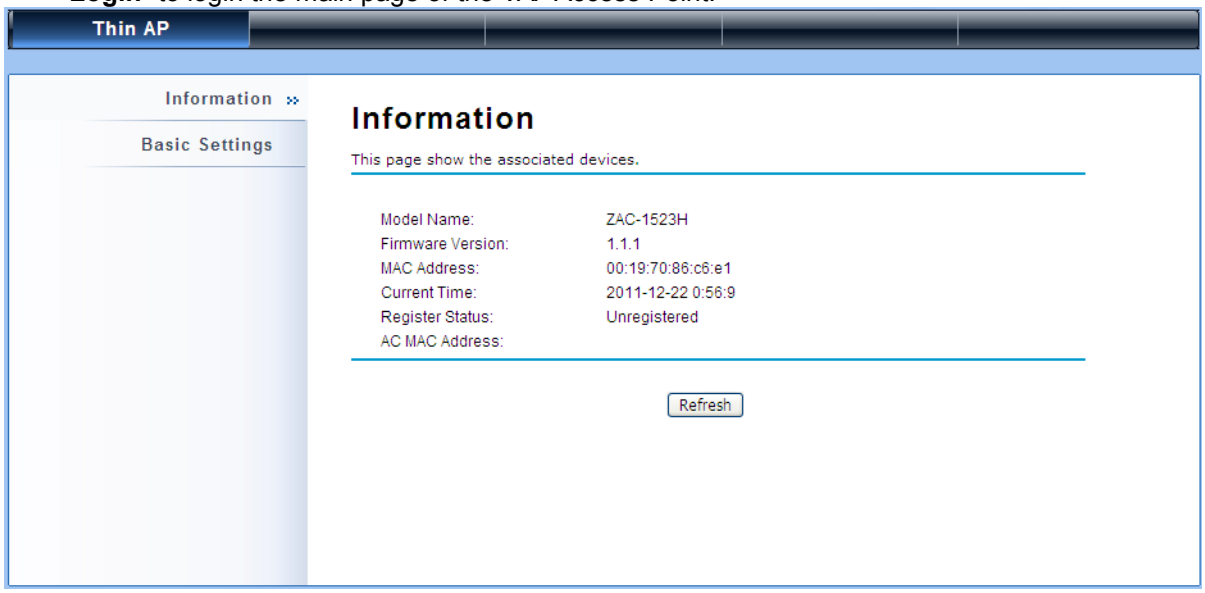
3. Chapter 3 Quick Start Tutorial

3.1. *Access the Web Configurator*

The VAP Access Point provides you with user-friendly Web-based management interface to easily manage the access point.

- Configure the computer with a static IP address of 192.168.1.x, as the default IP address of the VAP Access Point is 192.168.1.1. (X cannot be 0, 1, nor 255);
- Open Web browser and enter the IP address (Default: **192.168.1.1**) of the VAP Access Point into the address field. You will see the login page as below.

- Enter the username (Default: **admin**) and password (Default: **password**) respectively and click "**Login**" to login the main page of the VAP Access Point.



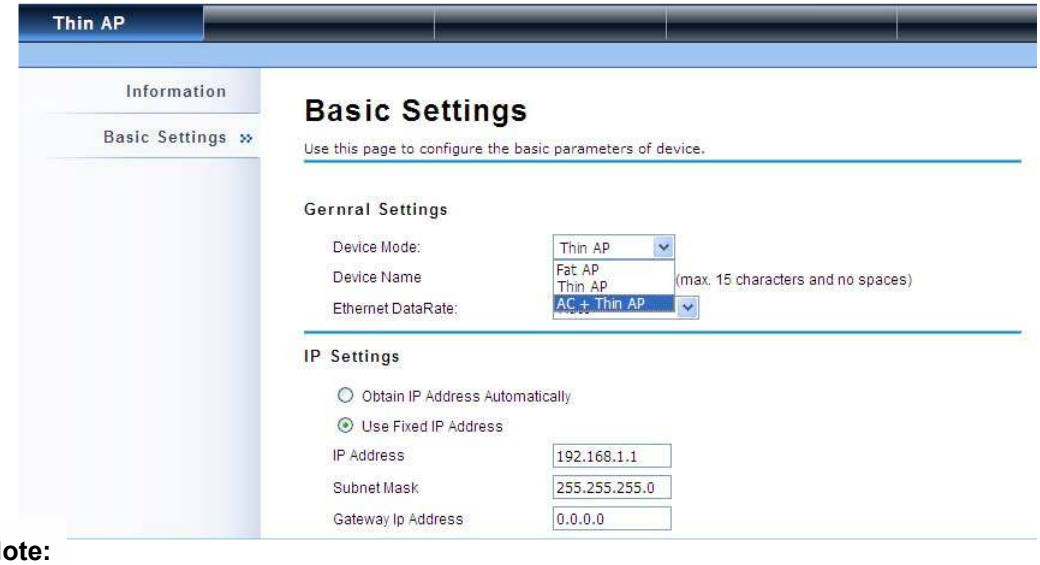
Note:

- The username and password are case-sensitive, and the password should be no more than 19 characters!

3.2. *Configure the AC+Thin AP mode*

The VAP Access Point covers "**Thin AP mode**", "**AC+Thin AP mode**", as well as "**FAT AP mode**". The default mode is Thin AP. To allow the VAP Access Point to manage the VAP-managed APs, you need to switch one of the VAP Access Points to AC+Thin AP mode first. To change it, please do the followings:

1. To operate as AC+Thin AP mode, go to **Basic Settings**. Assign an IP address for the VAP Access Point and from the **Device Mode** drop-down list, select "**AC+Thin AP**" and hit **YES** to make the change take effect.



Note:

- AC+ Thin AP mode allows the VAP Access Point to operate as access controller and thin AP concurrently.

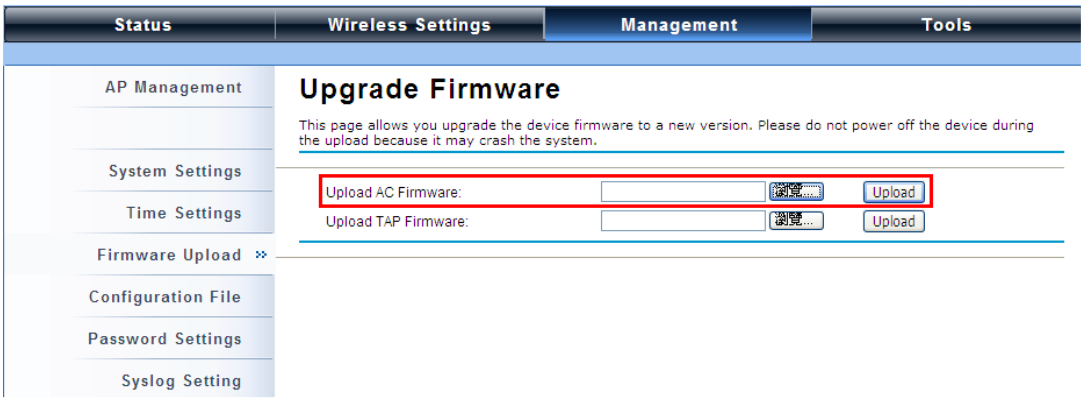
2. Assign an IP address to the VAP Access Point. It is strongly recommended not use the default password.

If you need to configure the wireless settings for the VAP Access Point especially SSID and encryption method, go to **Wireless Settings > Wireless Networks** and click on #1 **Wireless** SSID for configuration.

The wireless setting will also apply on the VAP-managed APs. A dialog message will pop up to apply changes to other VAP-managed APs. If the change only applies on the VAP Access Point in AC mode itself, you need to reboot the AP to make the settings take effect.

3.3. *Firmware Upgrade for VAP AP in AC mode*

To upgrade the firmware for the VAP Access Point in AC mode when necessary, go to **Management > Firmware Upload** and browse the firmware file where it is placed. Hit **Upload** to start the upgrade process. It will take approximately 3 minutes to complete the update.



3.4. *Install the VAP-Managed AP*

Install and connect the rest of VAP-managed Access Points to your network with the Ethernet cable. Power them up respectively. They will automatically discover the VAP Access Point in AC mode and issue registration request.

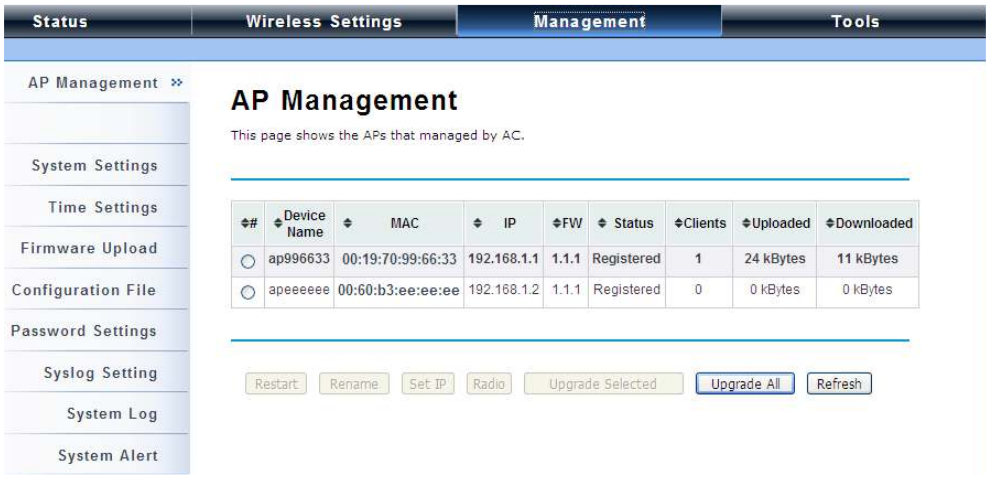
To check whether the thin APs are successfully registered or not, enter the web page of the VAP Access Point master access controller and go to **Management > AP Management**. You will see "**Registered**" in **Status** column. Besides registration status, you are able to see other information such as MAC address, IP address, FW version, number of clients that associate to each thin AP as well as upload/download speed.

Status
Wireless Settings
Management
Tools
AP Management
System Settings
Time Settings
Firmware Upload
Configuration File
Password Settings
Syslog Setting
AP Management
This page shows the APs that managed by AC.
| Device Name | MAC | IP | FW | Status | Clients | Uploaded | Downloaded
ap996633 | 00:19:70:99:66:33 | 192.168.1.1 | 1.1.1 | Registered | 1 | 24 kBytes | 11 kBytes
apeeeeee | 00:60:b3:ee:ee:ee | 192.168.1.2 | 1.1.1 | Registered | 0 | 0 kBytes | 0 kBytes
Restart
Rename
Set IP
Radio
Upgrade Selected
Upgrade All
Refresh

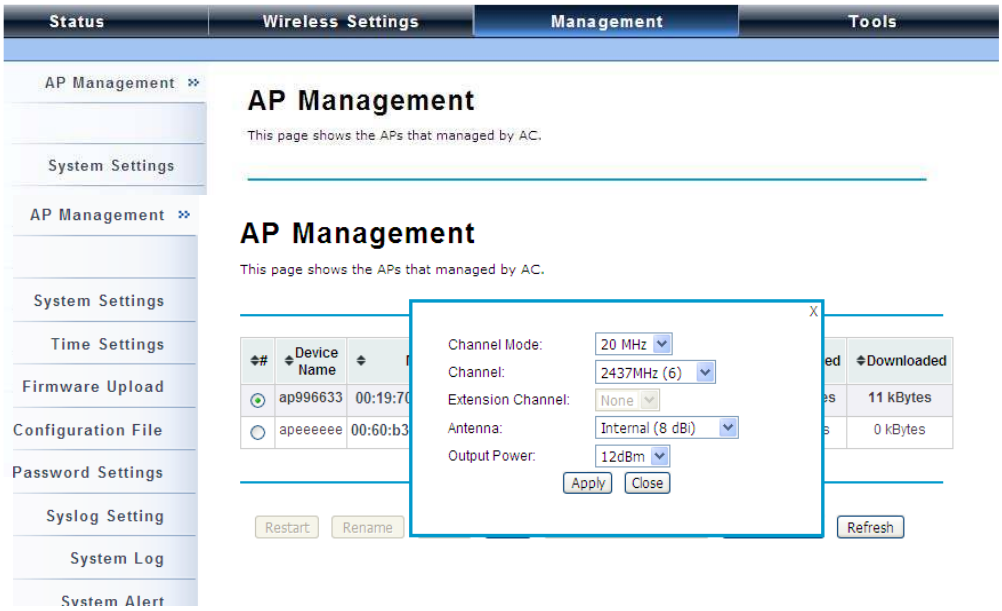
3.5. *Manage the VAP-managed APs*

To configure and manage the VAP-managed APs:

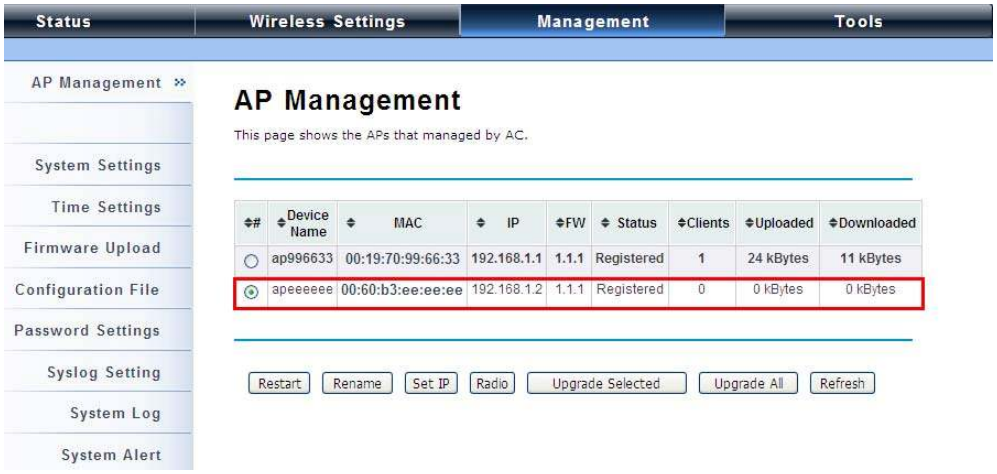
1. Enter the web page of the VAP Access Point in AC mode and go to **Management > AP Management**, the following screen shows up.



The VAP Access Point AP in AC+Thin mode on the list is highlighted in bold font. By selecting it and hit **Radio**, you may configure its radio setting such as **channel bandwidth**, **channel**, **antenna** and **output power**.



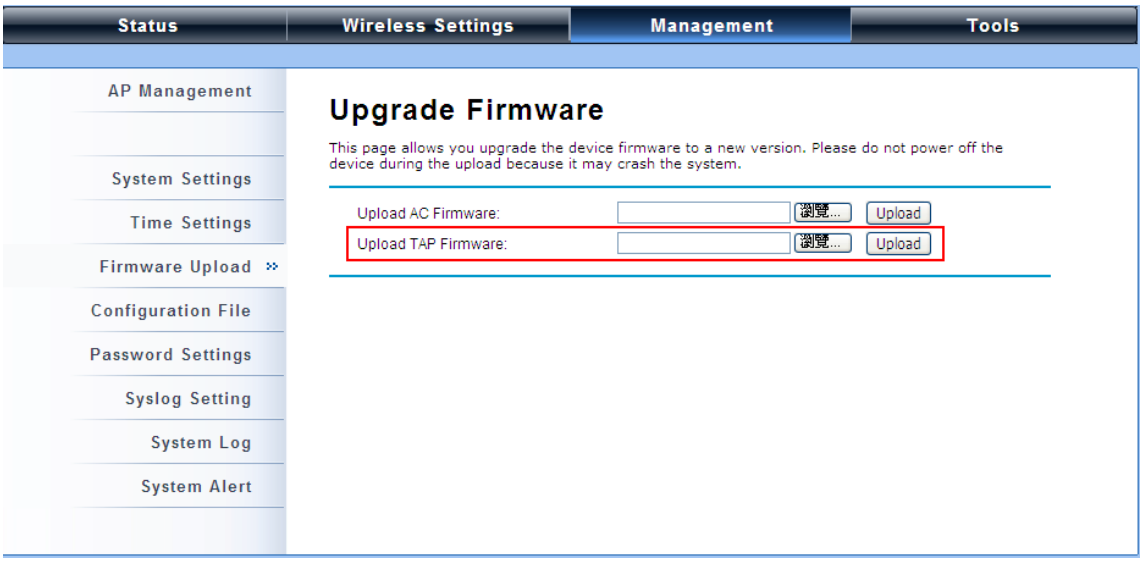
To configure other VAP-managed AP individually, select the one and hit the **Radio** button.

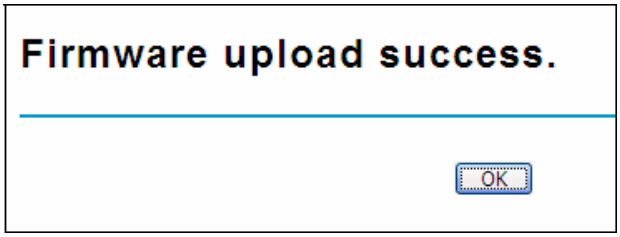


Besides radio setting, you may also reboot the VAP-managed AP, change its IP address and upgrade the firmware upgrade for VAP-Managed AP.

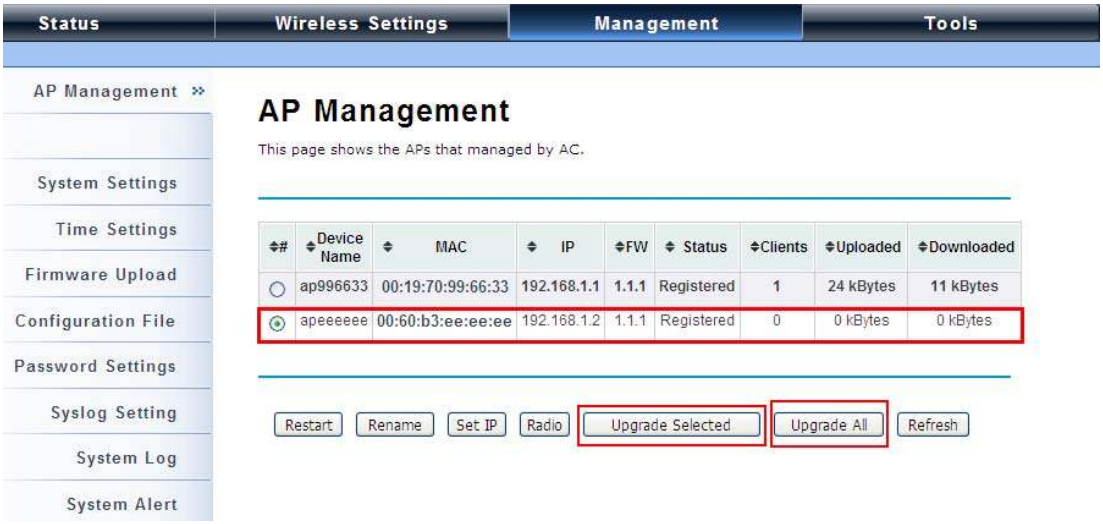
3.6. *Firmware Upgrade for VAP AP in AC mode*

For firmware upgrade, you may choose to upgrade the selected VAP-managed AP by hitting **Upgrade Selected**, or do the group upgrade by hitting **Upgrade All**.
Before upgrading the VAP-managed Access Point, you need to locate the new firmware in the VAP Access Point. Go to **Management > Firmware Upload**, browse the firmware file where it is located, click **Upload** and Click **OK**.



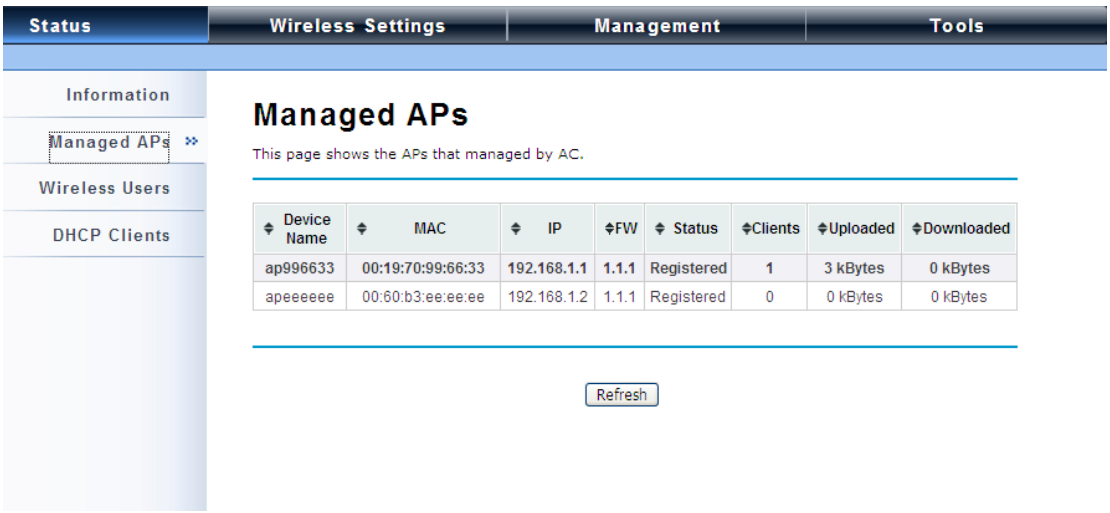


Then go back to **Management > AP Management to** do single or group update.



3.7. *Monitor the VAP-Managed AP*

To view each VAP-managed AP's status, please go to **Status > Managed APs**. Beside viewing device information such as device name, MAC address, IP address, and FW version, you may also monitor the wireless clients that are currently associated with the VAP-managed APs as well as packets statistics.

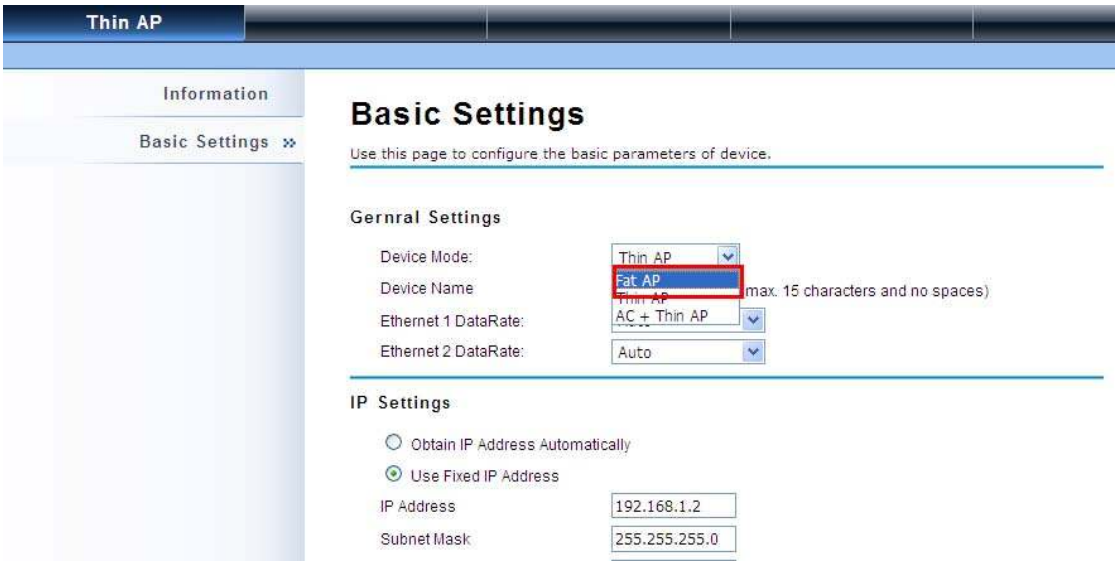


3.8. *Configure the Fat AP mode*

Fat AP mode operates as standalone AP that cannot be managed by the VAP Access Point.

For **VAP-Managed Acces Point in AC mode**, to configure it to **Fat AP** mode, go to **Management > System Settings**. From the **Device Mode** drop-down list, select "**Fat AP**" and hit **YES** to make the change take effect.

For **VAP-Managed AP**, enter the web page of the thin AP and go to **Basic Settings.** From the **Device Mode** drop-down list, select "**Fat AP**" and hit **YES** to make the change take effect.



The Fat AP covers “**AP mode**”, “**Wireless Client mode**”, “**Bridge mode**” as well as “**AP Repeater mode**”. For details please refer to the next Chapter.

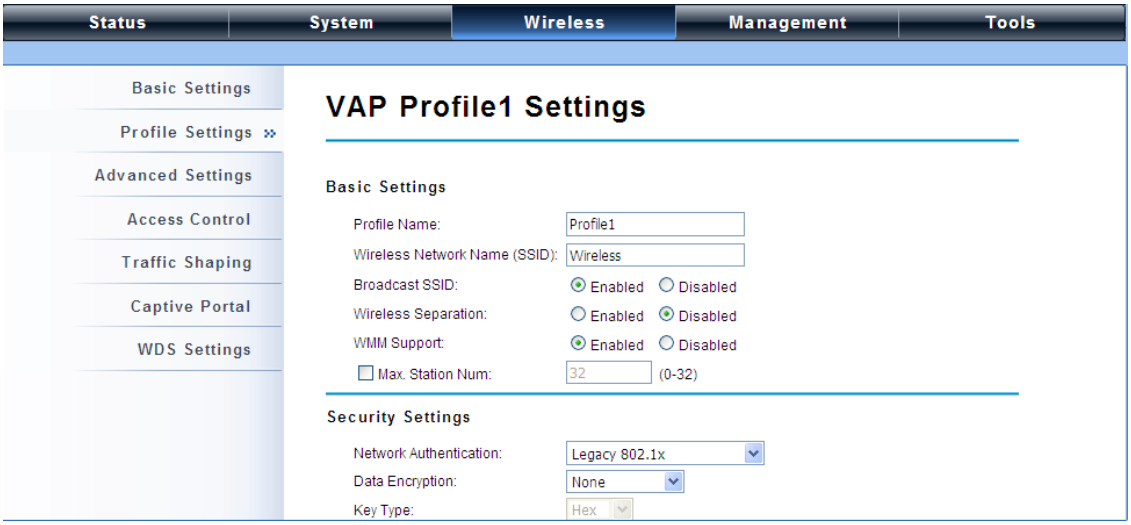
AP Mode

1. Choose **Wireless > Basic Settings**. The default is AP mode already. Here, you can set the parameters to optimize your application, or you can leave them as the default. Click **Apply** to save the parameters.

Note:

- In the example here, we only change the “Wireless Network Name (SSID)” as “Join_me”, and later, we will show you if AP mode works correctly. In addition, for better coverage of the AP, you may also use an external antenna; if so, remember to set the antenna setting from “Internal (8 dBi)” to “External (N-Type)” after your external antenna is successfully installed.
- To be reminded that you are able to choose “External (N-Type)” only when you have well done installing the external antenna; otherwise, it might cause damage the VAP itself.

2. If security is required, open **Wireless > Profile Setting** and enter “**VAP Profile 1 Settings**” as below. You may set the parameters like “Network Authentication” and “Data Encryption” for more secure network communication in your application. Click **Apply** to save the parameters.

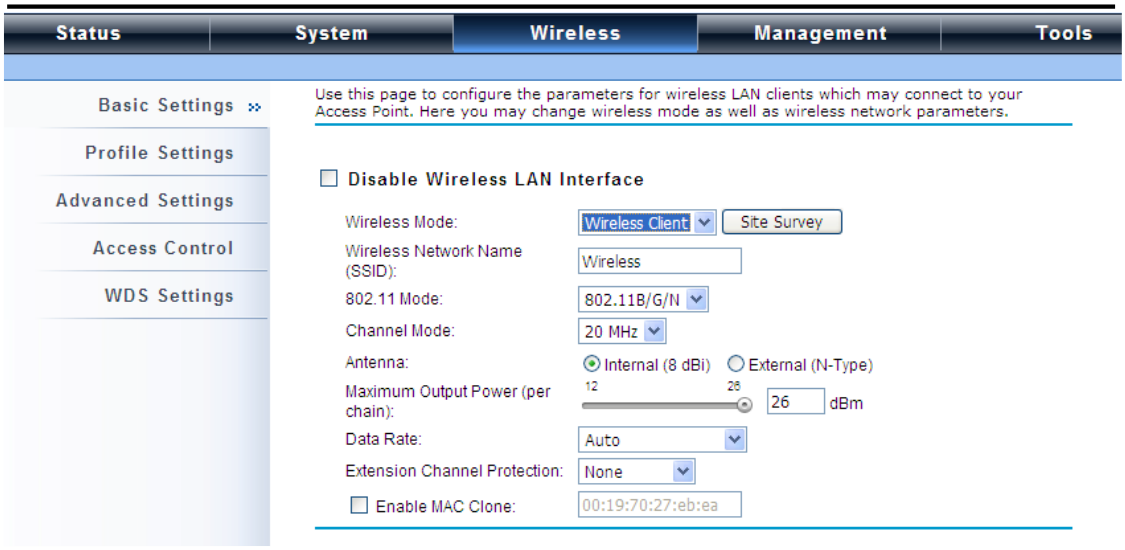


Wireless Client Mode

1. Choose **Wireless > Basic Settings**. Then you will see the "Wireless Basic Settings" page. Choose "**Wireless Client**" from Wireless Mode, and click **Apply** to save it. Feel free to change the other parameters to optimize your application before clicking **Apply**.

Note:

- For longer transmission, you may also use an external antenna; if so, remember to set the antenna setting from "Internal (8 dBi)" to "External (N-Type)" after your external antenna is successfully installed, otherwise **DO NOT** set to ""External (N-Type)" without physically attaching external antenna, otherwise, damage might be caused to the device itself.



2. Click the "**Site Survey"** button beside **Wireless Mode**. It will scan all the available access points within coverage. Select the one you prefer to connect to, and click **Selected** to establish the connection.

Wireless Site Survey

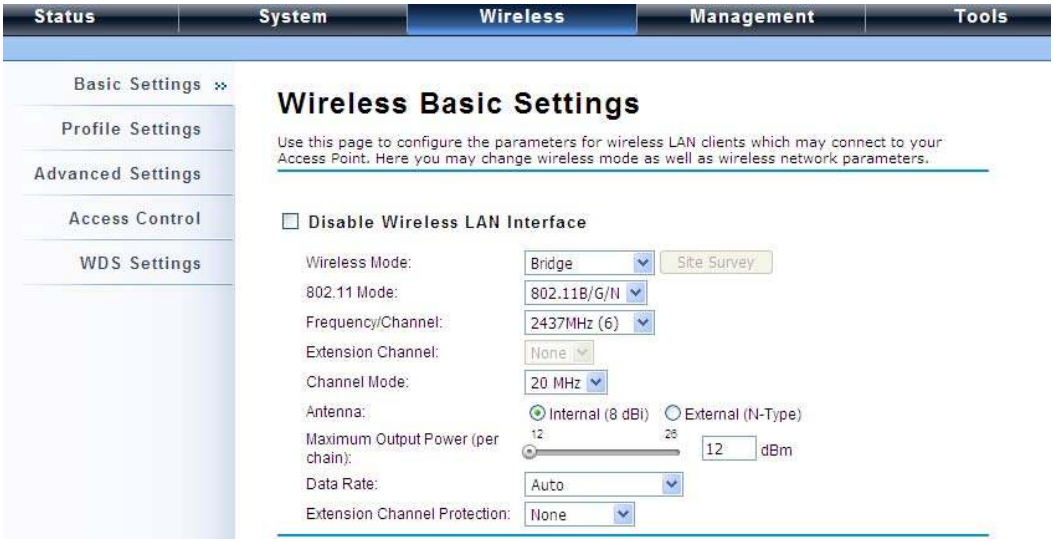
This page provides a tool to scan the wireless network.

Select	SSID	Frequency/Channel	MAC Address	Wireless Mode	Signal Strength	Security
◯	FAE_Test	2412MHz(1)	00:19:70:5b:fe:60	802.11B/G/N	-41	WPA2
◯	Cisco_1	2412MHz(1)	00:26:0a:ef:32:90	802.11B/G	-61	NONE
◯	Apple Network 873e69	2412MHz(1)	10:9a:dd:87:3e:69	802.11B/G/N	-77	WPA2
◯	AP2	2412MHz(1)	00:60:b3:47:9f:ce	802.11B/G	-86	WEP
◯	MIS-AP1	2462MHz(11)	00:19:70:79:e8:9b	802.11B/G	-41	WPA2
◯	MIS-AP1	2442MHz(7)	00:19:70:40:ff:f9	802.11B/G	-47	WPA2
◯	dd-wrt_G300N	2417MHz(2)	00:24:a5:b4:cf:77	802.11B/G	-76	WPA
◯	R2WAP64	2422MHz(3)	48:5b:39:bc:86:34	802.11B/G	-88	NONE
◯	MIS-AP1	2447MHz(8)	00:19:70:40:ff:fe	802.11B/G	-54	WPA2
◯	MIS-AP1	2452MHz(9)	00:19:70:40:ff:ff	802.11B/G	-63	WPA2

3. If the AP you connect to require authentication or encryption keys, click **Profile Settings** in the left column, fill out the corresponding items, and click " **Apply**" for data encryption.

Bridge Mode

1. Choose **Wireless > Basic Settings**. Then you will see the "Wireless Basic Settings" page. Choose "Bridge" from Wireless Mode, and click **Apply** to save it. Feel free to change the other parameters to optimize your application before clicking **Apply**.


Status
System
Wireless
Management
Tools
Basic Settings
Profile Settings
Advanced Settings
Access Control
WDS Settings
Wireless Basic Settings
Use this page to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless mode as well as wireless network parameters.
Disable Wireless LAN Interface
Wireless Mode: Bridge Site Survey
802.11 Mode: 802.11B/G/N
Frequency/Channel: 2437MHz (6)
Extension Channel: None
Channel Mode: 20 MHz
Antenna: Internal (8 dBi) External (N-Type)
Maximum Output Power (per chain): 12 28 12 dBm
Data Rate: Auto
Extension Channel Protection: None

2. Go to "**WDS Settings**" in "**Wireless**", input the MAC address of the remote bridge to "**Remote AP MAC Address 1**" field and click "**Apply**".

Status
System
Wireless
Management
Tools
Basic Settings
Profile Settings
Advanced Settings
Access Control
WDS Settings
WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC addresses of other APs which you want to communicate with in the table and then enable the WDS.This function can work only in Bridge and AP Repeater mode.
Local MAC Address: 00:19:70:00:fc:58
Remote AP MAC Address1: 00:19:70:00:00:01
Remote AP MAC Address2:
Remote AP MAC Address3:
Remote AP MAC Address4:

Note:

- Bridge uses the WDS protocol that is not defined as the standard thus compatibility issues between equipment from different vendors may arise. Moreover, Tree or Star shape network topology should be used in all WDS use-cases (i.e. if AP2 and AP3 are specified as the WDS peers of AP1, AP2 should not be specified as the WDS peer of AP3 and AP3 should not be specified as the WDS peer of AP2 in any case). Mesh and Ring network topologies are not supported by WDS and should be avoided in all the use cases.

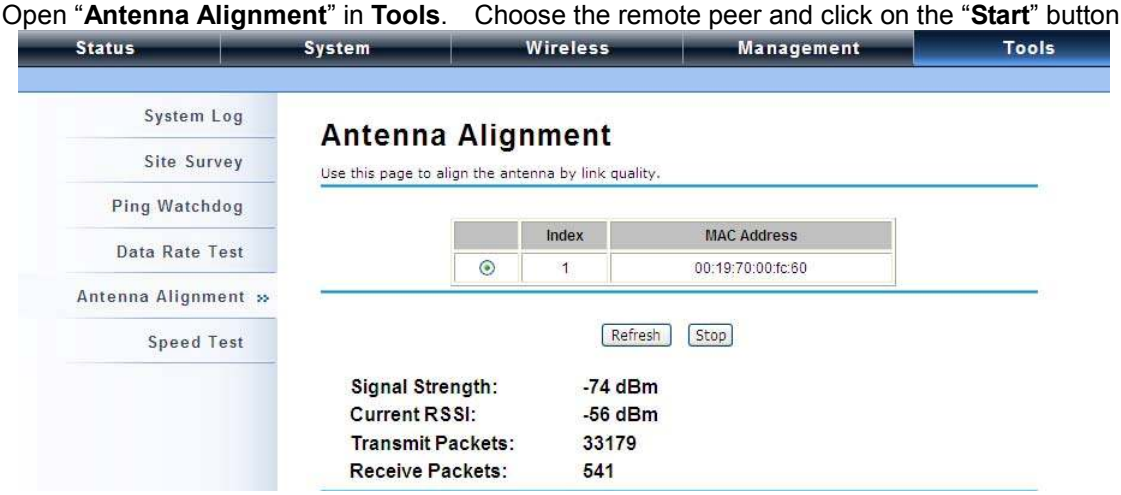
3. Repeat the above procedures to configure the remote VAP Access Point.

4. Enter the actual distance in **Space In Meter**. For example, if the distance between the two VAP bridges is 3 kilometers, enter 3000 in the field.

5. Use ping to check whether the link between the two bridges is OK.

6. To get a better wireless connectivity, antenna alignment is strongly recommended after both bridges are installed long distance apart.

7. Open "**Antenna Alignment**" in **Tools**. Choose the remote peer and click on the "**Start**" button.

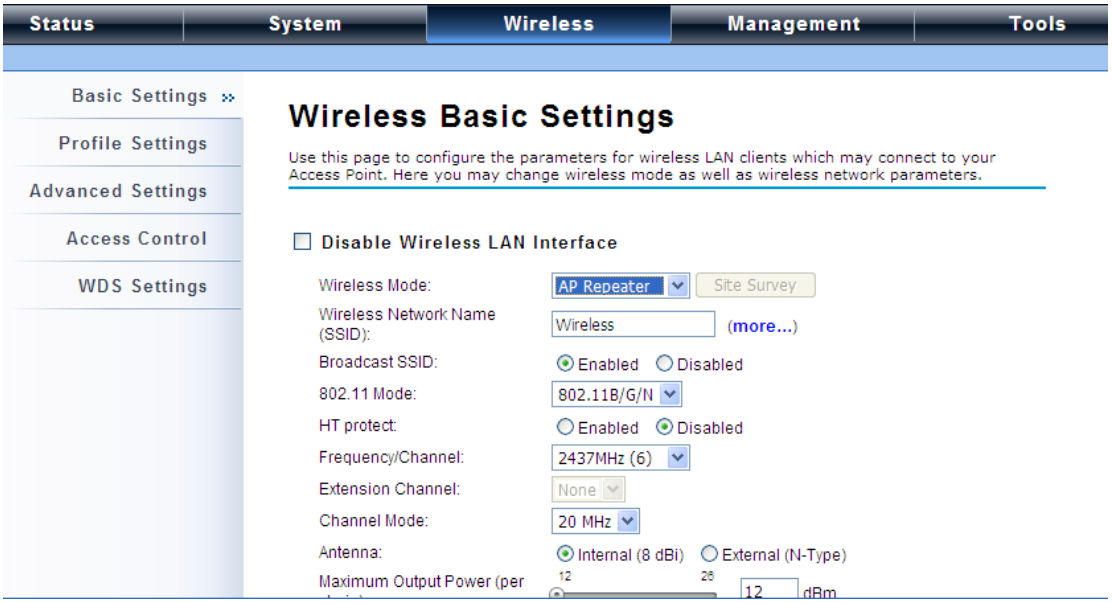


AP Repeater Mode

1. Choose **Wireless > Basic Settings**. Choose "**AP Repeater**" from Wireless Mode, and click **Apply** to save it. Feel free to change the other parameters to optimize your application before clicking **Apply**.

Note:

- For longer transmission of the VAP Access Point, you may also use an external antenna; if so, remember to set the antenna setting from "Internal (8 dBi)" to "External (N-Type)" after your external antenna is successfully installed, otherwise **do not** set to ""External (N-Type)" without external antenna, in case VAP Access Point has damage....



2. To establish point-to-point bridge connection, please follow the procedures described in Bridge mode. To connect the wireless client to the AP, please follow the procedures described in Wireless Client mode.

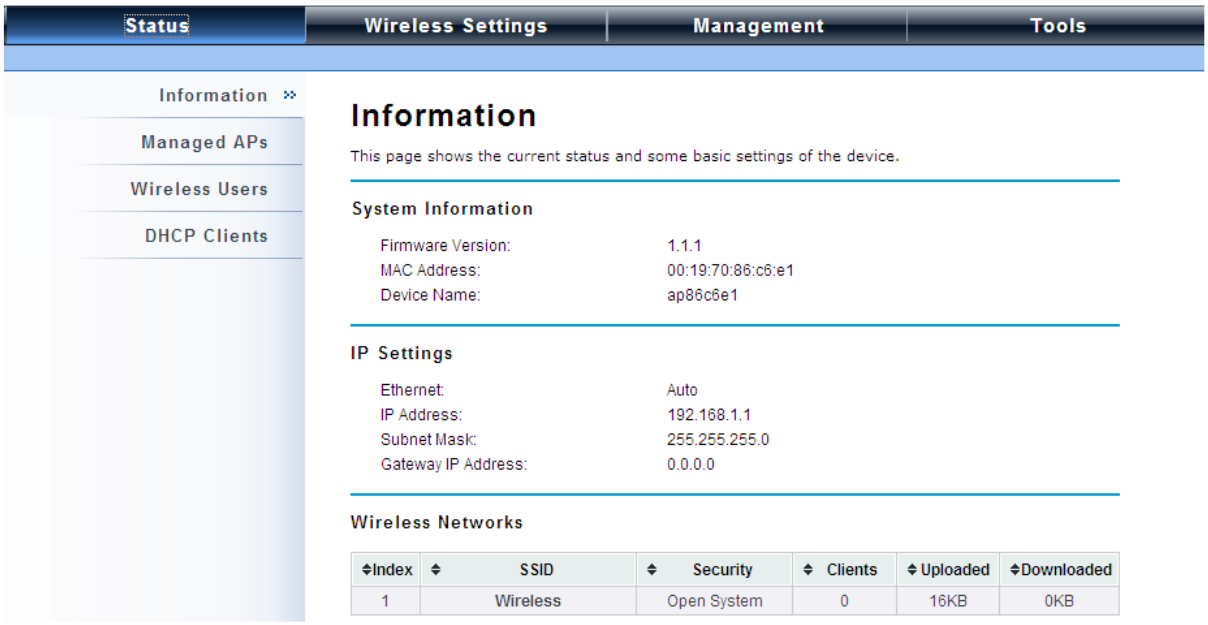
4. Chapter 4 Navigate the Web Configurator

4.1. *AC+Thin AP Mode*

4.1.1. Status

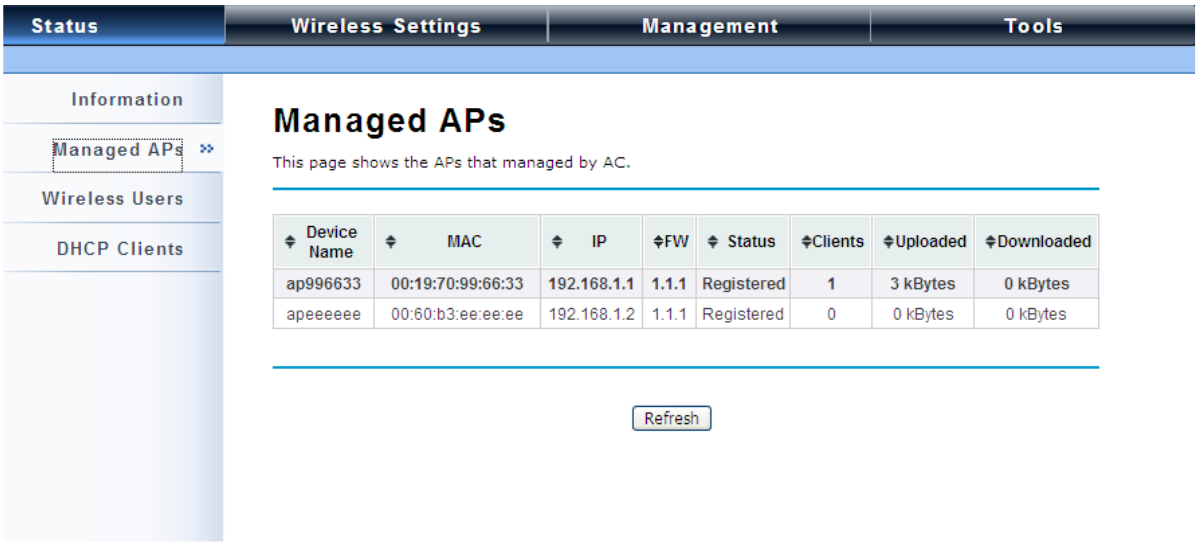
View Basic Information

Open "**Information**" in "**Status**" to check the basic information of the VAP Access Point, which is read only. Information includes system information, IP settings, and wireless network setting. Click "**Refresh**" at the bottom to have the real-time information.



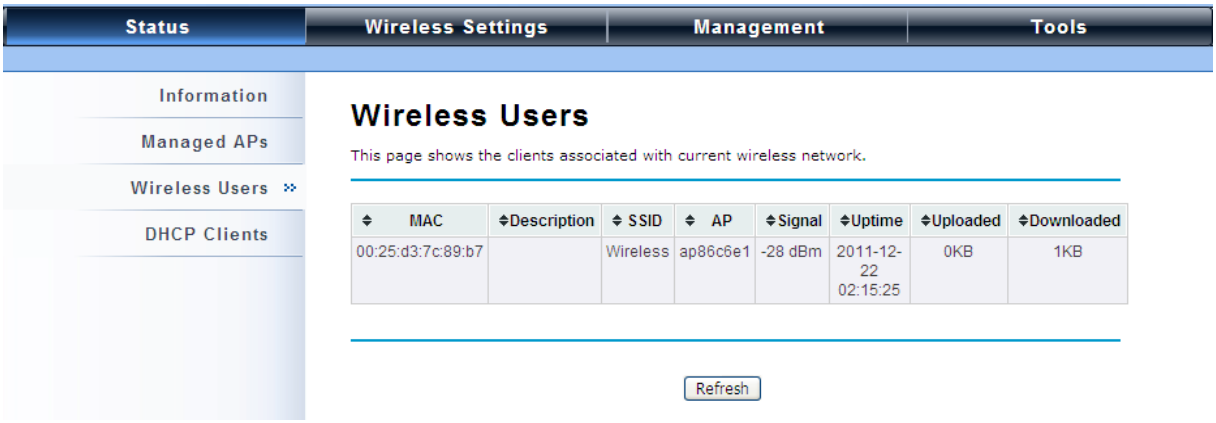
View VAP-Managed APs

Open "**Managed APs**" in "**Status**" to check information of managed AP such as device name, MAC address, IP address, numbers of associated clients and uploaded/downloaded packets. All is read only. Click "**Refresh**" at the bottom to update the list.



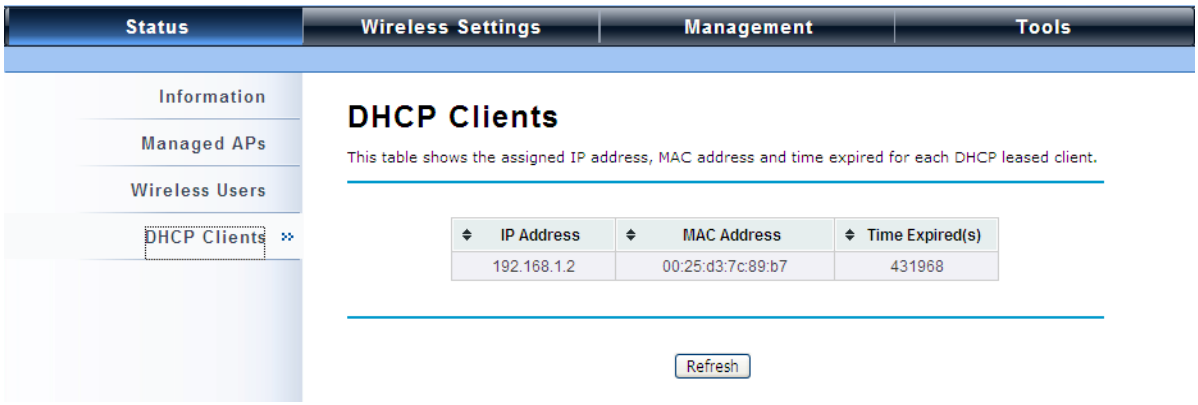
View Wireless Users

Open "**Wireless Users**" in "**Status**" to check the information of all the wireless clients such as MAC address, SSID of the VAP-managed AP that are associated with, signal strength, connection up time, and uploaded/downloaded packets. All is read only. Click "**Refresh**" at the bottom to update the list.



View DHCP Client Table

Open "**DHCP Clients**" in "**Status**" as below to check the assigned IP address, MAC address and lease time for each DHCP client. Click "**Refresh**" to update the table.



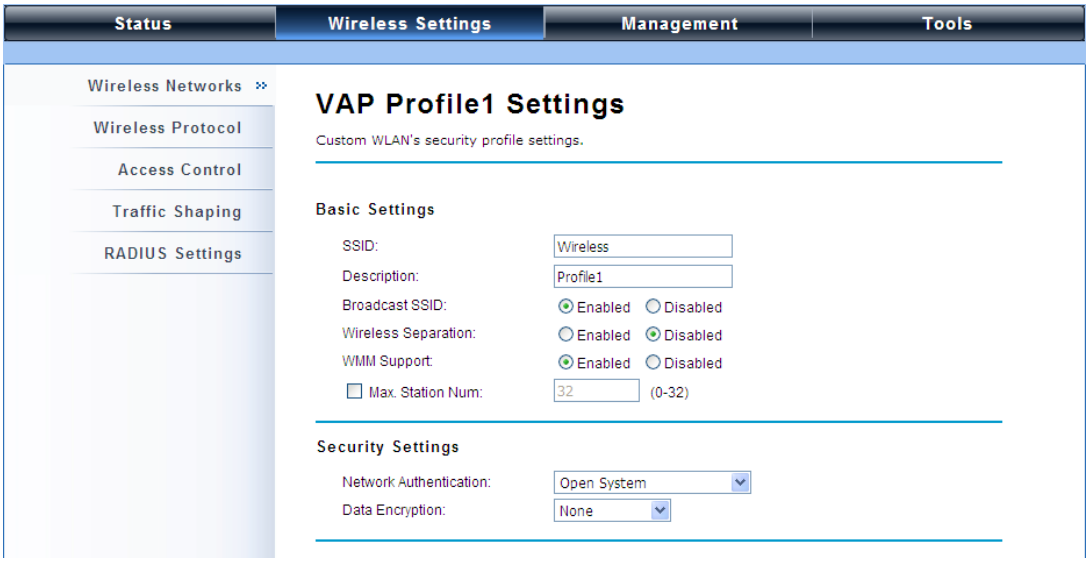
4.1.2. Wireless Settings

Wireless Setting allows you to configure wireless parameters, security method, access control and flow control for your VAP Access Point. Note that the configuration will also apply on all the other VAP-managed APs.

Wireless Networks (VAP Profiles Settings)

The VAP Access Point allows up to 16 virtual SSIDs on a single BSSID and to configure different profile settings such as security and VLAN ID to each SSID. To create a virtual AP, you may check the **Enable** box of the profile and click on the profile (eg. Profile 2) to configure wireless and security settings. Hit **Apply** to active the profile.

Status
Wireless Settings
Management
Tools
Wireless Networks
Wireless Protocol
Access Control
Traffic Shaping
RADIUS Settings
Wireless Networks
Define each WLAN's attribute.
Enable SSID Security VLAN ID Description
1 Wireless Open System 0 Profile1
2 Wireless Open System 0 Profile2
3 Wireless Open System 0 Profile3
4 Wireless Open System 0 Profile4
5 Wireless Open System 0 Profile5
6 Wireless Open System 0 Profile6
7 Wireless Open System 0 Profile7
8 Wireless Open System 0 Profile8
9 Wireless Open System 0 Profile9
10 Wireless Open System 0 Profile10



- **Basic Setting**

SSID: This wireless network name is shared among all associated devices in your wireless network. Keep it identical on all those devices. Note that the SSID is case-sensitive and cannot exceed 32 characters.

Description: Name of the VAP profile

Broadcast SSID: In AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA cannot scan and find the VAP Access Point, so that malicious attack by some illegal STA could be avoided.

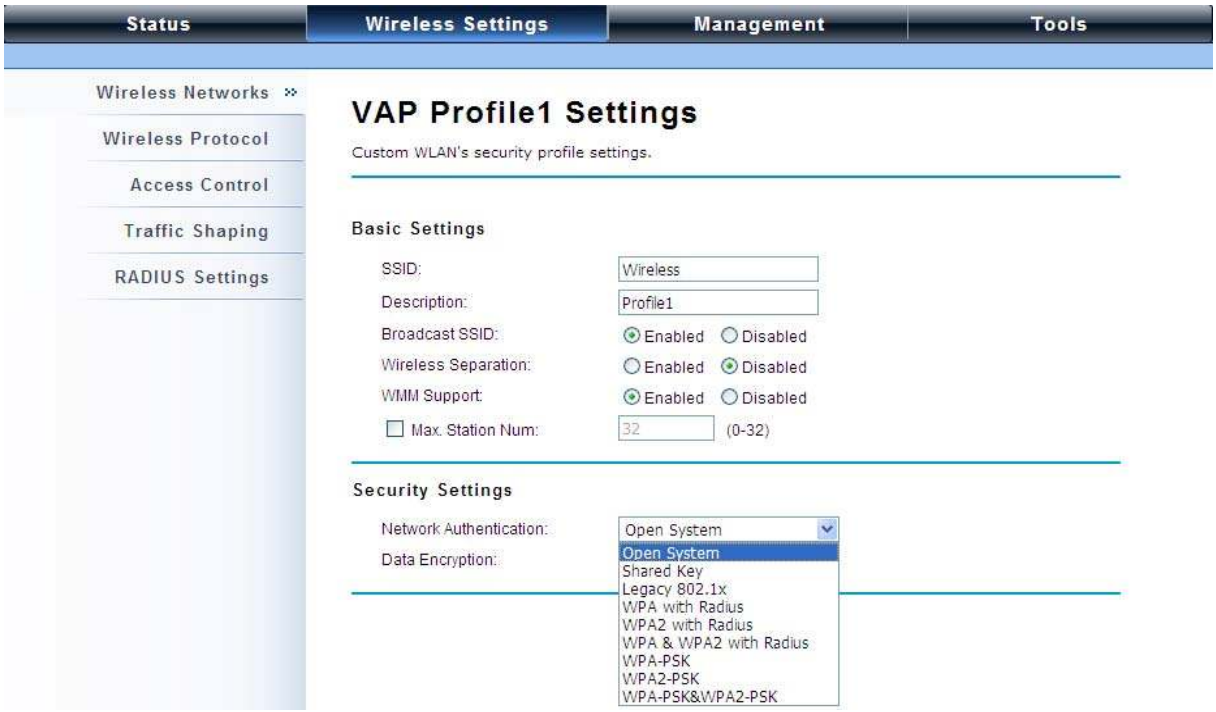
Wireless Separation: Wireless separation is an ideal way to enhance the security of network transmission. By enabling "**Wireless Separation**" can prevent the communication among associated wireless clients.

WMM Support: WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type under AP mode only, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should also support it. By default it is enabled and cannot be disabled in b/g/n mode.

Max. Station Number: By checking the "**Max. Station Num**" the VAP Access Point will only allow up to 32 wireless clients to associate with for better bandwidth for each client. By disabling the checkbox the AP will allow up to 128 clients to connect, but it is likely to cause network congestion or poor performance.

- **Security Setting:**

To prevent unauthorized radios from accessing data transmitting over the connectivity, the VAP Access Point provides you with rock solid security settings.



- **Network Authentication**

Open System: It allows any device to join the network without performing any security check.

Shared Key: Data encryption and key are required for wireless authentication (Not available in Bridge/AP Repeater mode).

Legacy 802.1x: It provides the rights to access the wireless network and wired Ethernet. With User and PC identity, centralized authentication as well as dynamic key management, it controls the security risk of wireless network to the lowest. To serve the 802.1x, at least one EAP type should be supported by the RADIUS Server, AP and wireless client.

WPA with RADIUS: Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. This is the common way to be adopted in large enterprise network.

WPA2 with RADIUS: WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. If it is selected, AES encryption and RADIUS server are required.

WPA&WPA2 with RADIUS: It provides options of WPA (TKIP) or WPA2 (AES) for the client. If it is selected, the data encryption type must be TKIP + AES and the RADIUS server must be set.

Note:

- If Radius relevant authentication type is selected, please go to **Wireless** □ **Radius Settings** for further radius server configuration.

WPA-PSK: It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.

WPA2-PSK: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.

WPA-PSK&WPA2-PSK: Available in AP mode, it provides options of WPA (TKIP) or WPA2 (AES) encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

- **Data Encryption**

If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.

None: Available only when the authentication type is open system.

64 bits WEP: It is made up of 10 hexadecimal numbers.

128 bits WEP: It is made up of 26 hexadecimal numbers.

152 bits WEP: It is made up of 32 hexadecimal numbers.

TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.

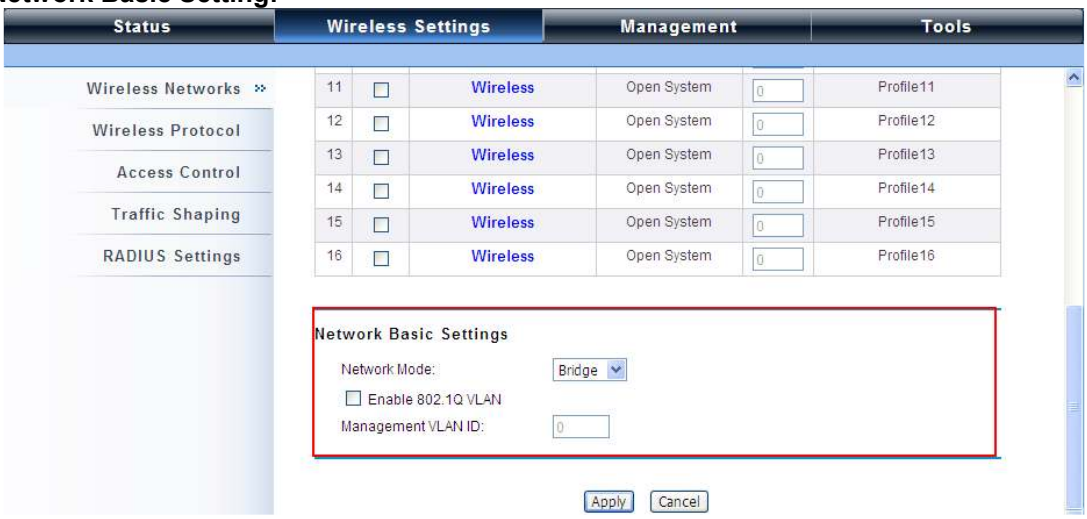
AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.

TKIP + AES: It allows for backwards compatibility with devices using TKIP.

Note:

- We strongly recommend you enable wireless security on your network!
- Only the same Authentication, Data Encryption and Key among the IEEE 802.11b/g/n VAP Access Point and wireless clients can the communication be established!

- **Network Basic Setting:**



Network Mode: Specify the network mode, including **Bridge** and **Router**. It is easy to configure parameters in Bridge Mode; however, users must pay extra attention to the way they configure the device when it is set to Router Mode.

VLAN: Available in Bridge AP mode, if your network uses VLANs, you can assign one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN. To allow users on the VLAN to access the WEB page of the VAP Access Point, you need to enable "**Enable 802.1Q VLAN**" and assign a management VLAN ID for your device. Make sure the assigned management VLAN ID is identical to your network VLAN ID to avoid failures of accessing the VAP AP's web page.

4.1.3. Wireless Protocols

Allow the user to change country code, 802.11 mode and other advanced parameters for the VAP Access Point.

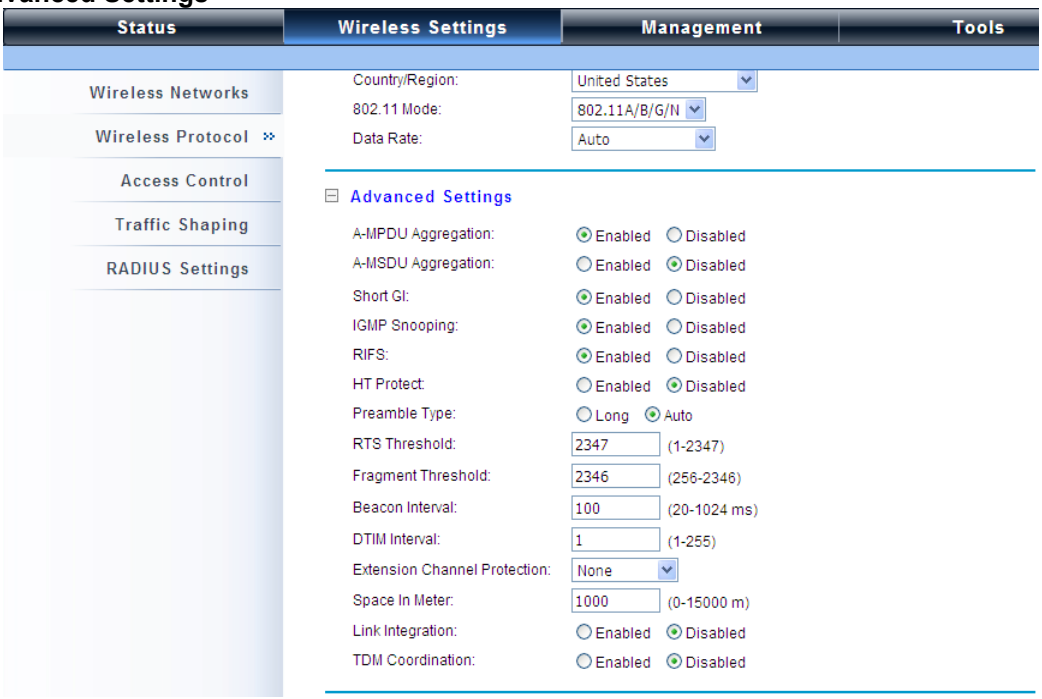
- **Basic Settings**

Country Region: The availability of some specific channels and/or operational frequency bands is country dependent.

802.11 Mode: The VAP Access Point can communicate with wireless devices of 802.11b/g or 802.11b/g/n.

Data Rate: Usually "**Auto**" is preferred. Under this rate, the VAP Access Point will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance by fixing the data rate.

- **Advanced Settings**



A-MPDU/A-MSDU Aggregation: The data rate of your AP except wireless client mode could be enhanced greatly with this option enabled; however, if your wireless clients don't support A-MPDU/A-MSDU aggregation, it is not recommended to enable it.

Short GI: Under 802.11n mode, enable it to obtain better data rate if there is no negative compatibility issue.

IGMP Snooping: IGMP snooping is the process of listening to IGMP network traffic. By enabling IGMP snooping, the AP will listen to IGMP membership reports, queries and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group.

RIFS: RIFS (Reduced Interframe Spacing) is a means of reducing overhead and thereby increasing network efficiency

HT Protect: Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.

Preamble Type: It defines some details on the 802.11 physical layer. "**Long**" and "**Auto**" are available.

RTS Threshold: The VAP Access Point sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in byte. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

Fragmentation Threshold: Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

Beacon Interval: Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024.

DTIM Interval: DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.

Extension Channel Protection Mode: This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

Space in Meter: To decrease the chances of data retransmission at long distance, the VAP Access Point can automatically adjust proper ACK timeout value by specifying distance of the two nodes.

Link Integration: Available under AP mode, it monitors the connection on the Ethernet port by checking "**Enabled**". It can inform the associating wireless clients as soon as the disconnection occurs.

TDM Coordination: Stands for “Time-Division Multiplexing Technique”, this resource reservation control mechanisms can avoid packet collisions and send the packets much more efficiently allowing for higher effective throughput rates. This function is only available in AP mode. It is highly recommended to enable TDM coordination when there are multiple VAP ACCESS POINTs needed to connect to the AP in your application.

4.1.4. Access Control

The Access Control appoints the authority to wireless client on accessing VAP Access Point, thus a further security mechanism is provided. This function is available only under AP/Router mode.

Open “**Access Control**” in “**Wireless Settings**” as below.

Status
Wireless Settings
Management
Tools
Wireless Networks
Wireless Protocol
Access Control
Traffic Shaping
RADIUS Settings
Wireless Access Control
If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.
Wireless Network:
VAP1 - Wireless
Access Control Mode:
Deny Listed
MAC Address:
Apply
Cancel
MAC Address Select Edit
1 00:19:70:86:c6:e3 Edit
Delete Selected
Delete All
Refresh

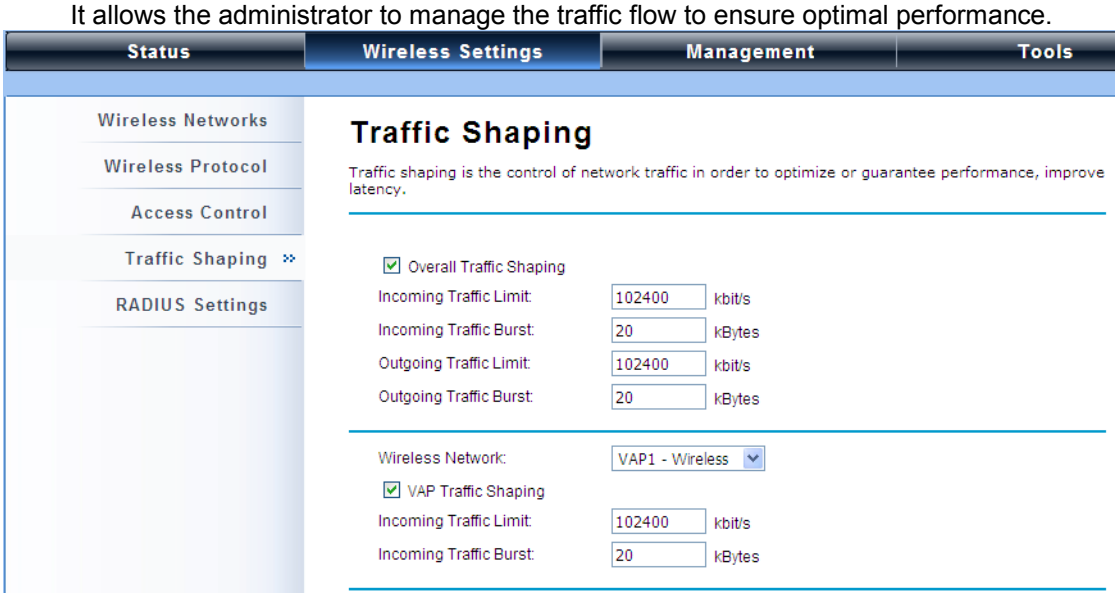
- **Wireless Network:** Select the VAP network you would like to enable access control.
- **Access Control Mode**
  If you select “**Allow Listed**”, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your AP. While when “**Deny Listed**” is selected, those wireless clients on the list will not be able to connect the AP.
- **MAC Address**
  Enter the MAC address of the wireless client that you would like to list into the access control list, click “**Apply**” then it will be added into the table at the bottom.

- **Delete Selected/All**

  Check the box before one or more MAC addresses of wireless client(s) that you would like to cancel, and click "**Delete Selected**" or "**Delete All**" to cancel that access control rule.

4.1.5. Traffic Shaping

It allows the administrator to manage the traffic flow to ensure optimal performance.



- **Overall Traffic Shaping**

  Check this box to control the overall bandwidth of the VAP Access Point.

  Incoming Traffic Limit: To specify maximum incoming bandwidth to a certain rate in kbit/s.

  Incoming Traffic Burst: To specify the buffer size for incoming traffic that can be sent within a given unit of time. The suggested value is 20KBytes. You may just leave the default value there, and then the connection will be bound to the traffic shaping rule at all times. You may decrease it to smaller value if the incoming traffic limit is smaller.

  Outgoing Traffic Limit: To limit the outbound traffic to a certain rate in kbit/s.

  Outgoing Traffic Burst: To specify the buffer size for outbound traffic. The suggested value is 20KBytes. You may decrease it to smaller value if the outbound traffic limit is smaller.

- **VAP Traffic Shaping**

  Check this box to control the overall bandwidth for a specific VAP network.

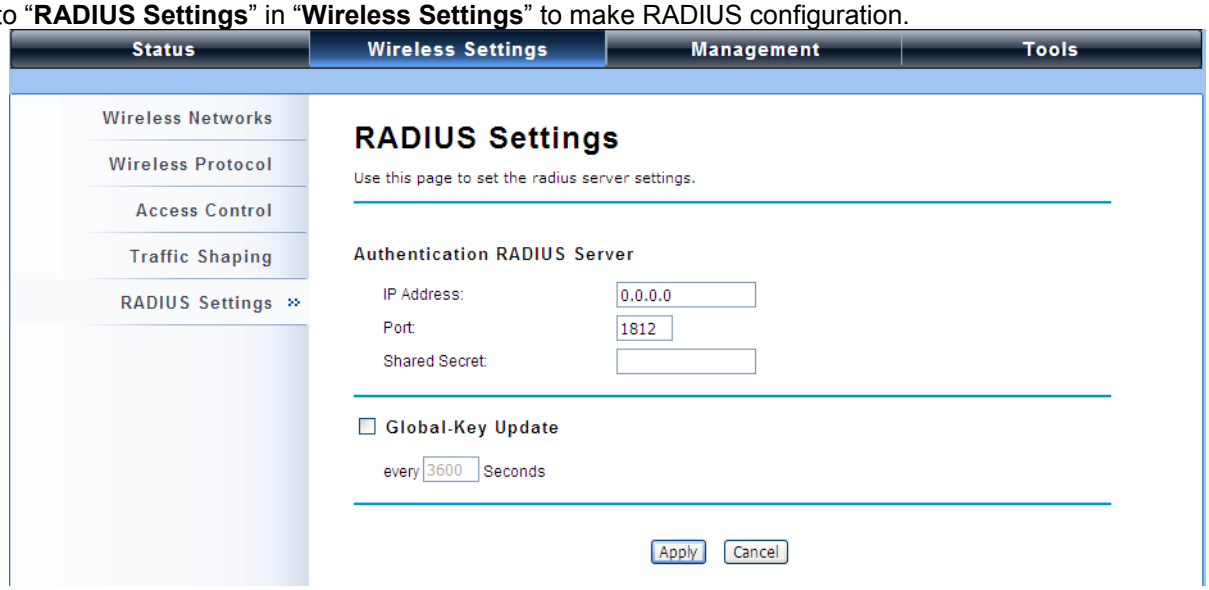
  Incoming Traffic Limit: To specify maximum incoming bandwidth to a certain rate in kbit/s.

  Incoming Traffic Burst: To specify the buffer size for incoming traffic that can be sent within a given unit of time. The suggested value is 20KBytes. You may just leave the default value there, and then the connection will be bound to the traffic shaping rule at all times. You may decrease it to smaller value if the incoming traffic limit is smaller.

4.1.6. Radius Settings

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; playing a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share. If 802.1X, WPA(2) is used, you need to configure radius settings.

Go to “**RADIUS Settings**” in “**Wireless Settings**” to make RADIUS configuration.



- **Authentication RADIUS Server**
  This is for RADIUS authentication. It can communicate with RADIUS through IP Address, Port and Shared Secret.

  IP Address: Enter the IP address of the Radius Server;

  Port: Enter the port number of the Radius Server;

  Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the VAP Access Point and RADIUS during authentication.

- **Global-Key Update**
  Check this option and specify the time interval between two global-key updates. Default is 3600 seconds.

4.1.7. TCP/IP Settings

When the Router mode is activated, the **TCP/IP Settings** will show up in **Wireless Settings** for user to configure the TCP/IP for the VAP-managed Access Point.

Status
Wireless Settings
Management
Tools
Wireless Networks
Wireless Protocol
Access Control
Traffic Shaping
RADIUS Settings
TCP/IP Settings
Captive Portal
Firewall Settings
TCP/IP Settings
This page configures the Thin APs' IP address , subnet mask, DHCP, and other parameters at the ath for your local area network that is connected to the LAN port of the device.
LAN Settings :
IP Address : 192.168.0.99
Subnet Mask : 255.255.255.0
DHCP Server : Enabled
DHCP IP Address Range : 192.168.0.1 - 192.168.0.200
DHCP Subnet Mask : 255.255.255.0
Lease Time : 7200 (15-44640 Minutes)

- **LAN Settings:**

IP Address: Specify the IP address for the VAP-managed Access Point.

Subnet Mask: Specify the Subnet mask for the VAP-managed Access Point.

DHCP Server: Select to enable or disable DHCP server on the VAP-managed Access Point.

DHCP IP Address Range: When the DHCP Server is enabled, users may specify DHCP IP Address Range for the VAP-managed Access Point.

DHCP Subnet Mask: Specify the DHCP Subnet Mask for the VAP-managed Access Point.

Lease Time: Specify the lease time (15-44640 minutes) for the VAP-managed Access Point.

Note:

- For wireless clients who want to access the unit's web page in Router mode, please type the IP address here in the browser's address bar to enter the web page.

4.1.8. Captive Portal

Captive portal is a management which allows WLAN users to easily and securely access the Internet. Under Router mode, when captive portal is enabled, the VAP Access Point will redirect the client to go to an authentication web page before browsing Internet web pages. Captive portals are used on most Wi-Fi hotspots networks. Therefore, to use captive portal, you need to find the service providers that have the additional services needed to make captive portal work.

To enable Captive Portal, check "**Captive Portal**" and select the VAP network needed for captive portal.

- **Radius Settings**

  Primary Radius Server: Enter the name or IP address of the primary radius server

  Secondary Radius Server: Enter the name or IP address of the primary radius server if any.

  Radius Auth Port: Enter the port number for authentication

  Radius Acct Port: Enter the port number for billing

  Radius Shared Secret: Enter the secret key of the radius server

  Radius NAS ID: Enter the name of the radius server if any

- **Radius Administrative-User:**

  Radius Admin Username: Enter the username of the Radius Administrator

  Radius Admin Password: Enter the password of the Radius Administrator

- **Captive Portal**

  UAM Portal URL: Enter the address of the UAM portal server

  UAM Secret: Enter the secret password between the redirect URL and the Hotspot.

4.1.9. Firewall Settings

The firewall is a system or group of systems that enforce an access control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. The VAP Access Point has capabilities of Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding as well as DMZ. This is available only under **Router** Mode.

- **Source IP Filtering:**

You may create and activate a rule that filters a packet based on the source IP address from your local network to Internet. Check "**Enable Source IP Filtering**" to activate rule.

Local IP Address: Enter the IP address you would like to restrict.

Comment: Make comments to record your filtering rule.

Click **Apply** and the IP address will be added in the list. To delete the IP address from filtering, click **Select** checkbox of the designated IP address and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

Destination IP Filtering:

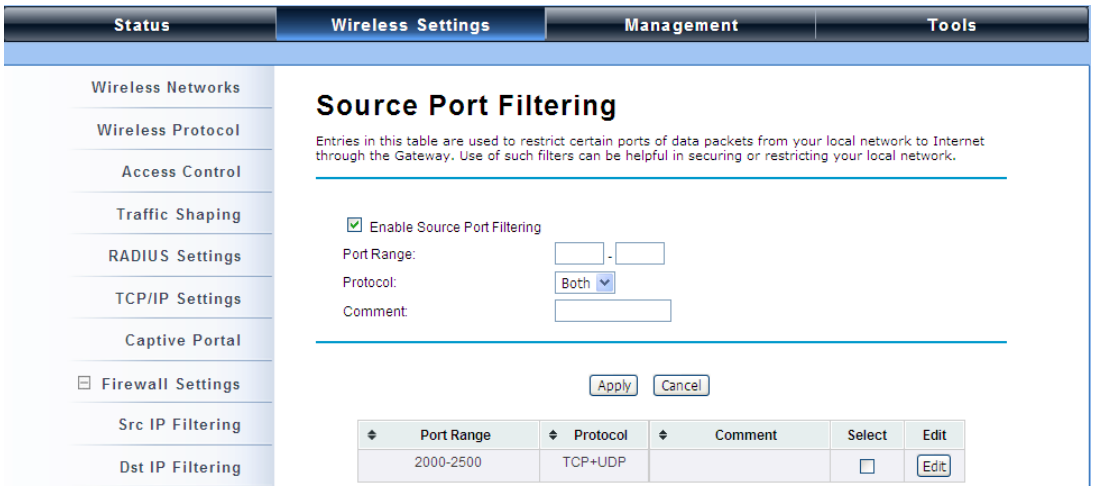
You may create and activate a rule that filters a packet based on the destination IP address to restrict the local computers from accessing certain websites. Check "**Enable Destination IP Filtering**" to activate rule.

Destination IP Address: Enter the IP address to be restricted.

Comment: Make comments to record your filtering rule.

Click **Apply** and the IP address will be added in the list. To delete the IP address from filtering, click **Select** checkbox of the designated destination IP address and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

- **Source Port Filtering:**



You may create and activate a rule that filters a packet based on the source port from your local network to Internet. Check "**Enable Source Port Filtering**" to activate rule.

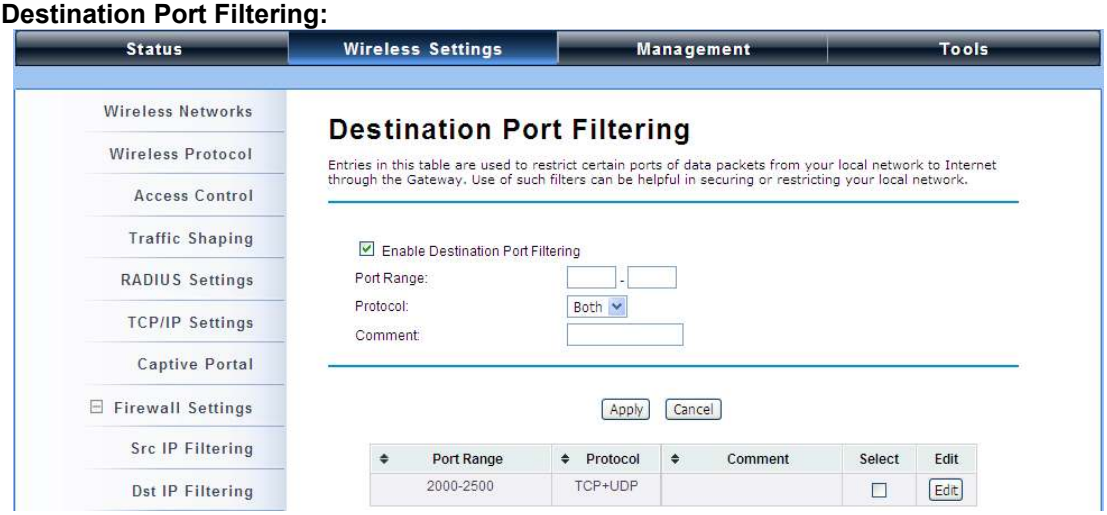
Port Range: Enter the port range you would like to restrict.

Protocol: Select port protocol: **Both**, **TCP**, **UDP**.

Comment: Make comments to record your filtering rule.

Click **Apply** and the IP address will be added in the list. To delete the restricted source ports, click **Select** checkbox of the designated ports and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

- **Destination Port Filtering:**



You may create and activate a rule that filters a packet based on the destination port from your local network to Internet. Check "**Enable Destination Port Filtering**" to activate rule.

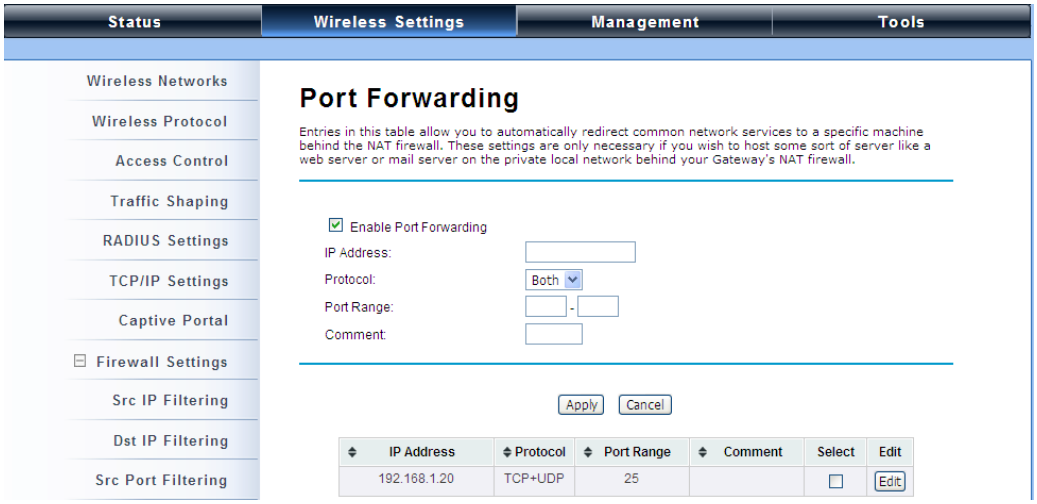
Port Range: Enter the port range you would like to restrict.

Protocol: Select port protocol: **Both**, **TCP**, **UDP**.

Comment: Make comments to record your filtering rule.

Click **Apply** and the IP address will be added in the list. To delete the restricted destination ports, click **Select** checkbox of the designated ports and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

- **Port Forwarding:**



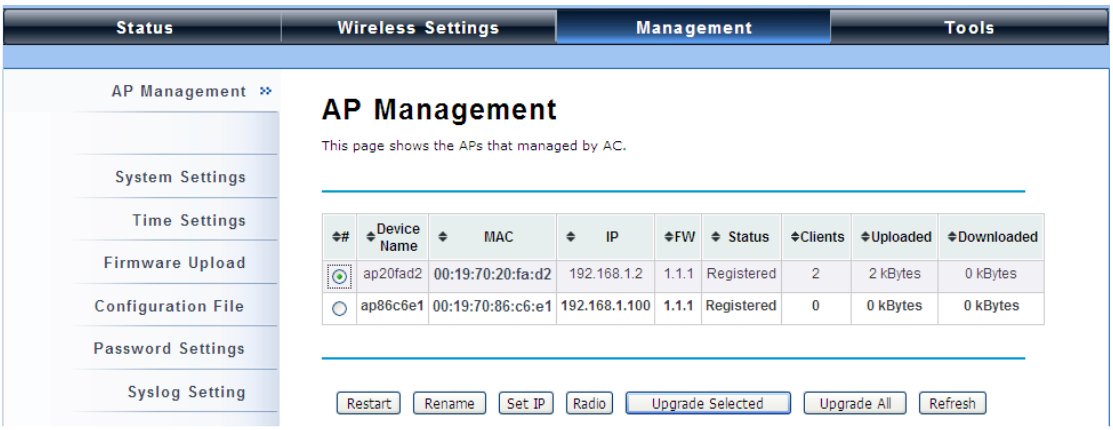
The port forwarding allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings ne are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind IEEE 802.11b/g/n Wireless VAP Access Point's NAT firewall.

4.1.10. Management

The VAP Access Points can manage up to 50 VAP-managed APs. The VAP Access Point provides thin AP management for editing the VAP-managed AP settings, upgrading the firmware and monitoring, etc.

AP Management

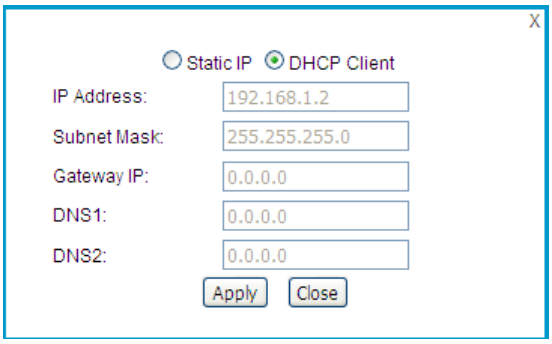
AP Management allows you to configure and upgrade the VAP-managed APs. Select the VAP-managed AP you would like to specifically configure.



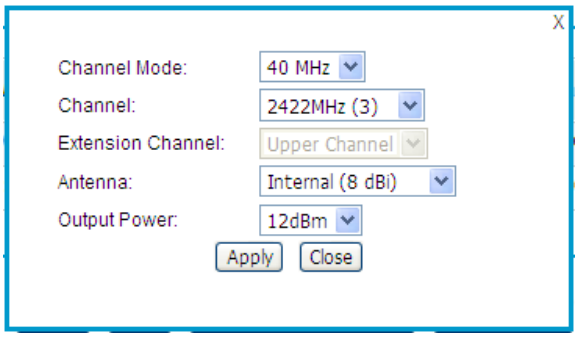
Restart: Restart the selected VAP-managed AP.

Rename: Rename for the selected VAP-managed AP.

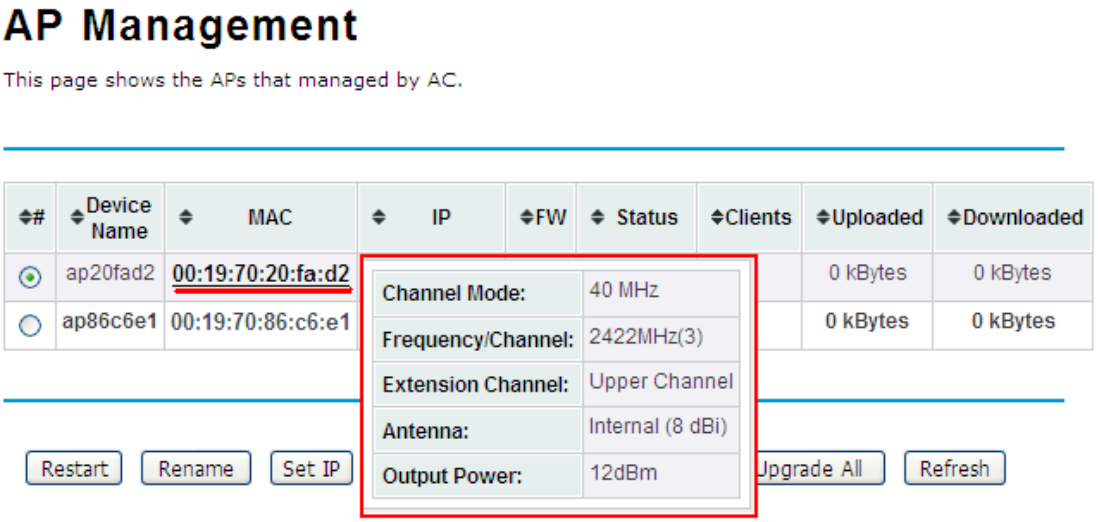
Set IP: Assign a static IP address for the selected VAP-managed AP or obtain the IP address from VAP Access Point in AC mode. Default is DHCP client.



Radio: Allows to configure the channel bandwidth, operating channel, antenna and output power for the selected VAP-managed Access Point.



From the AP Management list, move the mouse cursor to the MAC address of the selected VAP-managed AP the screen will pop up radio configuration information.



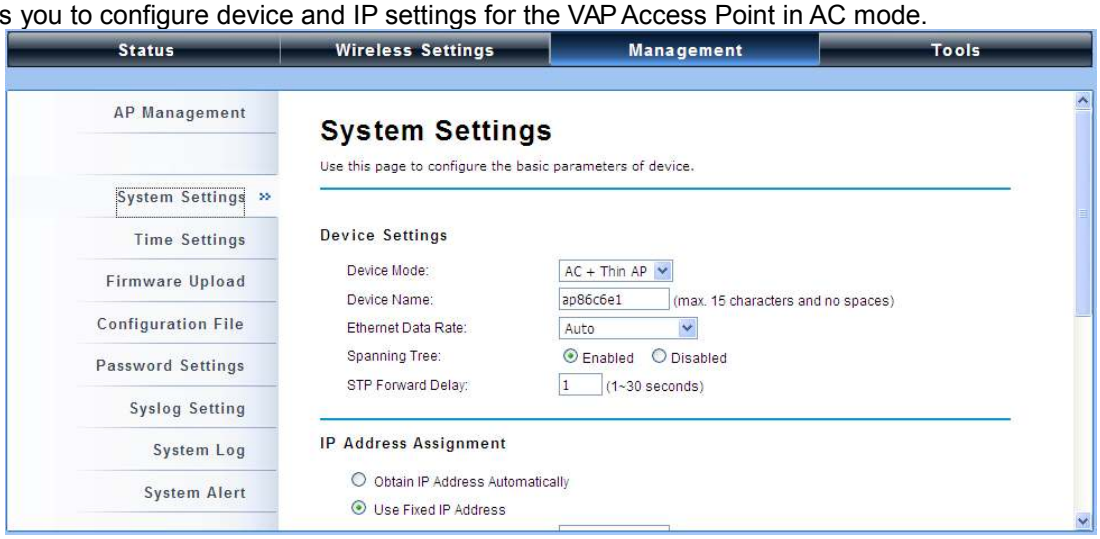
Upgrade Selected: Upgrade firmware for the selected VAP-managed AP. Note that you need to upload the firmware file into the VAP Access Point in AC mode prior to firmware upgrade, otherwise a window will pop up saying TAP firmware hasn't been uploaded.

Upgrade All: Click to upgrade all the VAP-managed APs simultaneously.

Refresh: Refresh the AP management list manually.

System Settings

Allows you to configure device and IP settings for the VAP Access Point in AC mode.



- **Device Settings:**

  Device Mode: Three modes are provided: **AC+Thin AP**, **Thin AP**, **FAT AP**. Select AC+Thin AP to have the device act as virtual access controller to manage other VAP-managed APs on your network. Select "Thin AP" to have the VAP Access Point managed by the VAP AP in AC mode. Select FAT AP to perform as a standalone AP, neither managing nor managed by other VAP APs.

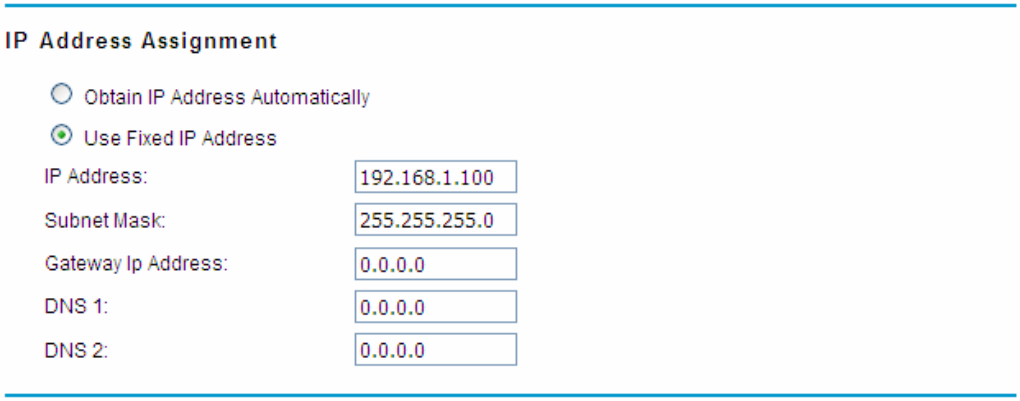
  Device Name: Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).

  Ethernet Data Rate: Specify the transmission rate of data for Ethernet. Default is **Auto**.

  Spanning Tree: Spanning Tree Protocol (STP) is a link management protocol for AP which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the access points but establish the redundant link as a backup if the initial link fails.

  STP Forward Delay: STP Forward Delay is the time spent in detecting and learning network tree topology state before entering the forward state. Default time value is 1 sec.

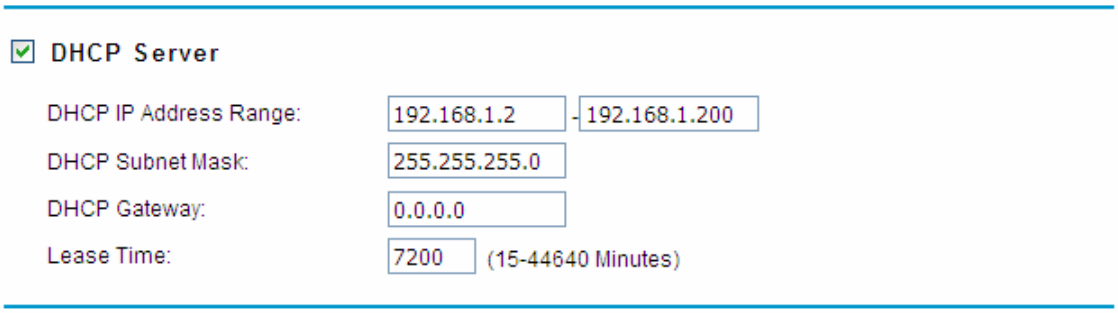
- **IP Address Assignment:**



Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option, thus the VAP Access Pioint is able to obtain IP settings automatically from the DHCP server.

Use Fixed IP Address: Check this option. You have to specify a static IP address, subnet mask, default gateway and DNS server for the VAP Access Point manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

- **DHCP Server**
  The VAP Access Point in AC mode can perform a DHCP server to assign IP address to the VAP-managed APs. Default is enabled.


DHCP Server
DHCP IP Address Range: 192.168.1.2 - 192.168.1.200
DHCP Subnet Mask: 255.255.255.0
DHCP Gateway: 0.0.0.0
Lease Time: 7200 (15-44640 Minutes)

DHCP IP Address Range: Specify the IP range.

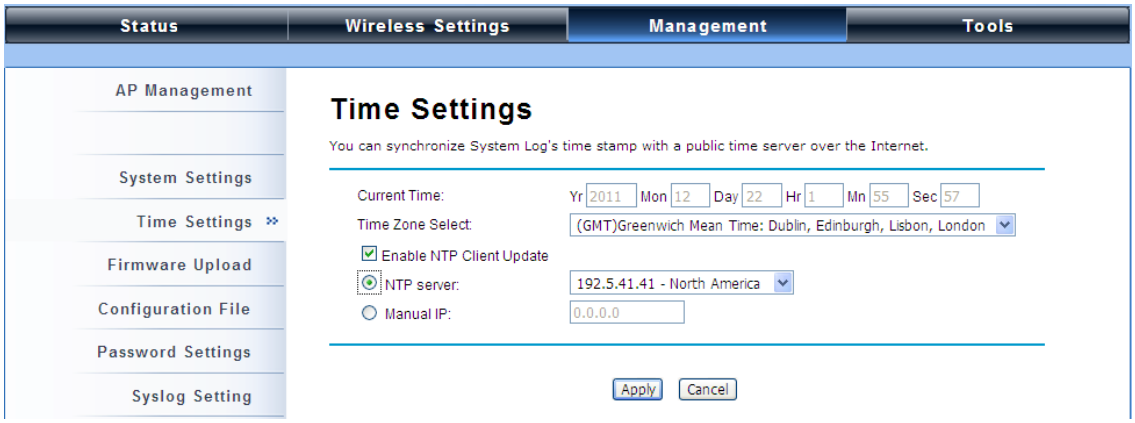
DHCP Subnet Mask: Specify the DHCP Subnet Mask.

DHCP Gateway: Specify the gateway address.

Lease Time: Specify the DHCP lease time.

Time Settings

Compliant with NTP, the VAP Access Point is capable of keeping its time in complete accord with the Internet time. To use this feature, check "**Enable NTP Client Update**" in advance.



- **Current Time**
  Display the present time in Yr, Mon, Day, Hr, Min and Sec.

- **Time Zone Select**
  Select the time zone from the dropdown list.

- **NTP Server**
  Select the time server from the "**NTP Server**" dropdown list. or manually input the IP address of available time server into "**Manual IP**".

Firmware Upgrade

Besides upgrading firmware for the VAP Access Point in AC mode, it also provides firmware update for the VAP-managed APs.

- **Upload AC Firmware:** Allows the network administrator to upgrade firmware for the VAP Access Point in AC mode.

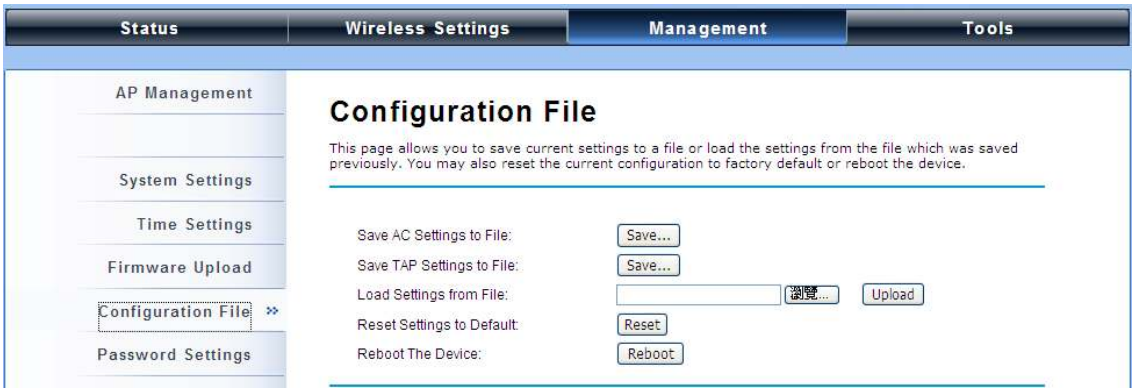
- **Upload TAP Firmware:** Before updating the firmware for the VAP-managed APs, you need to upload the firmware into the VAP Access Point in AC mode that allows the virtual controller AP to do the firmware upgrade for VAP-managed APs.

Note:

- Do NOT cut the power off during upgrade, otherwise the system may crash!

Backup/ Retrieve Settings

It is strongly recommended you back up configuration information in case of something unexpected. If tragedy hits your device, you may have an access to restore the important files by the backup. All these can be done by the local or remote computer.



- **Save AC Settings to File**
  Click **Save** to export the configuration file of VAP Access Point in AC mode. Then the configuration file **ac.cfg** will be generated and saved to the specified location.

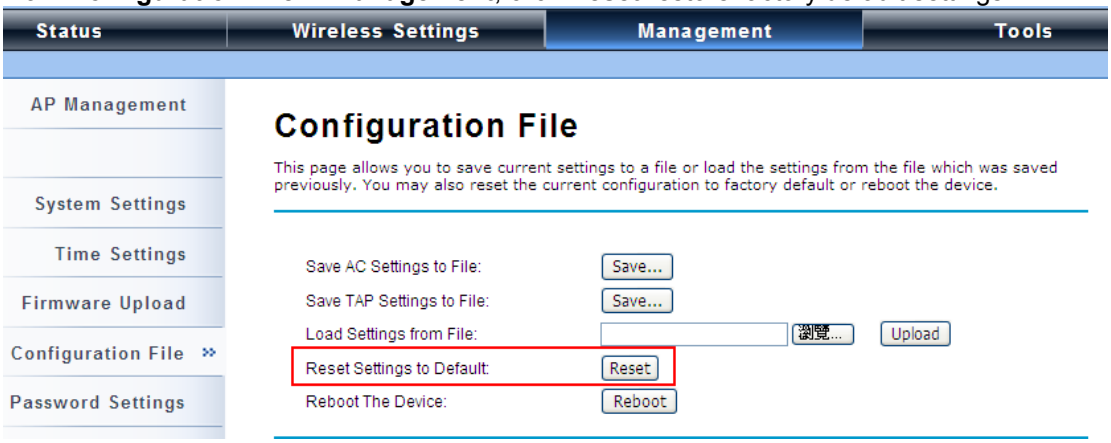
- **Save TAP Settings to File**
  Click **Save** to export the configuration file of VAP-managed AP. Then the configuration file **tap.cfg** will be generated and saved to the specified location.

- **Load Settings from File**
  Import **ac.cfg** load into the VAP Access Point in AC mode.

Restore Factory Default Settings

The VAP Access Point provides two ways to restore the factory default settings:

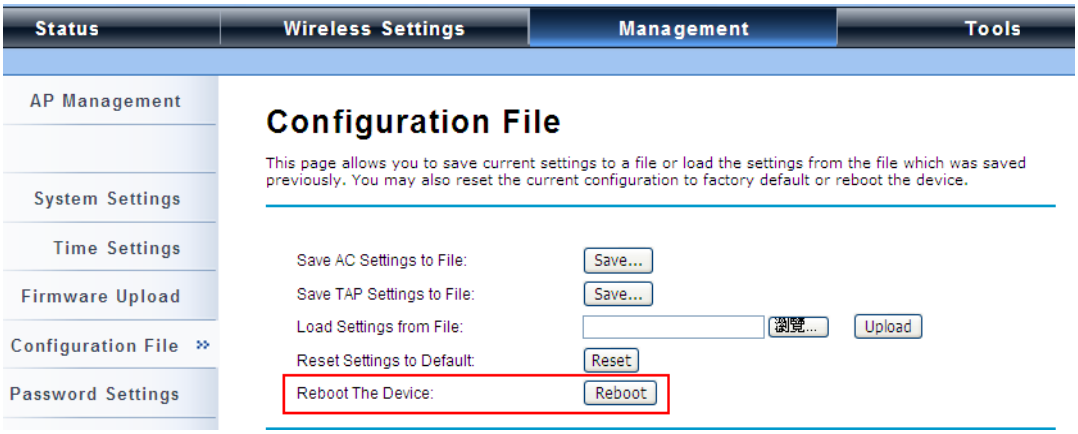
- **Restore factory default settings via Web**
  From **Configuration File** in **Management**, click **Reset** restore factory default settings.



- **Restore factory default settings via Reset Button**
  If software in VAP Access Point is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via the reset button. Press and hold the button for at least 5 seconds and then release it until the PWR LED gives a blink. The hardware reset will take about 2 minutes to complete.

Reboot

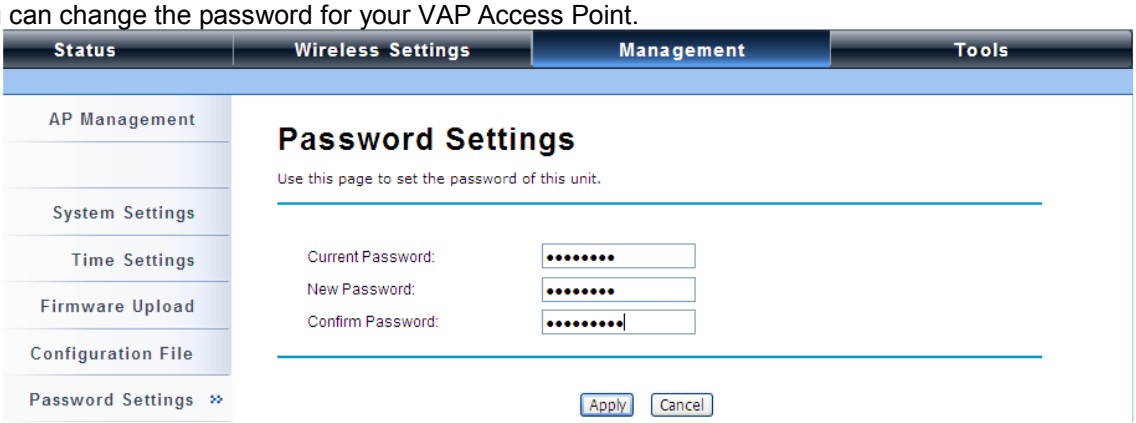
You can software reboot your VAP Access Point from **Configuration File** in **Management** as below:



Click "**Reboot**" and hit "**Yes**" upon the appeared prompt to start reboot process. This takes a few minutes.

Password Settings

You can change the password for your VAP Access Point.



- **Current Password**: Enter the current password.
- **New Password:** Enter the new password.
- **Confirm Password:** Enter the new password again for confirmation.

Note:

- The password is case-sensitive and its length cannot exceed 19 characters!

Syslog Setting:

The VAP Access Point provides remote syslog management by sending logs to an external syslog server. The log can be also sent through Email.

- **Remote Syslog Server**

  Enable Remote Syslog: Enable to send log to remote syslog server.

  IP Address: Specify the IP address of the remote server.

  Port: Specify the port number of the remote server.

- **Send Syslog via Email**

  Log Schedule: Configure the frequency of logs being sent. 5 scheduling options are provided:

  Never, **Hourly**, **Daily**, **Weekly**, and **When log is full**.

  Severity Level: Choose **All** to send all the logs or **Alert** to send only the alert messages.

  Send Log to: Specify the email address where you would like to send the log.

  Day for Sending Log: When Weekly scheduling is selected, you may specify which week day to send the log.

  Time for Sending Log: Specify the time of the day to send the log.

  Clear Log: To clear log after sending logs via email, check the **After Sending Mail** checkbox.

- **Mail Server Setting**

  Send Log From: Enter the email address of the mail server.

  Mail Subject: Type a title to be presented in the subject line of the log email message.

  SMTP Server: Enter the IP address of the SMTP sever.

  SMTP Authentication: If you want to use SMTP authentication, check **SMTP Authentication ,**checkbox and enter the user account and password.

System Log:

System log record and display all logs and alert message in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted. You may click **Clear** to delete logs manually as well.

Status
Wireless Settings
Management
Tools
AP Management
System Settings
Time Settings
Firmware Upload
Configuration File
Password Settings
Syslog Setting
System Log
System Alert
System Log
This page show the system log.
Time Priority Source Message
1 2011-12-22 00:55:05 info 192.168.1.100 znmpd: AC started.
2 2011-12-22 00:55:06 alert 00:19:70:86:C6:E1 WLAN service started.
3 2011-12-22 00:55:06 alert 00:19:70:86:C6:E1 WLAN service stopped.
4 2011-12-22 00:55:06 alert 00:19:70:86:C6:E1 WLAN service started.
5 2011-12-22 00:55:11 alert 192.168.1.100 znmpd: Device connected.
6 2011-12-22 00:55:12 notice 192.168.1.111 WEB: Authorized user "admin".
7 2011-12-22 00:55:41 alert 192.168.1.2 znmpd: Device connected.
8 2011-12-22 01:36:47 alert 00:60:B3:11:22:33 Station reassociated.
9 2011-12-22 01:39:47 alert 00:60:B3:11:22:33 Station deauthenticated.
10 2011-12-22 02:15:06 notice 192.168.1.111 WEB: User "admin" logout.

System Alert:

System alert record and events occurred on both VAP Access Point in AC mode and VAP-managed AP in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted. You may click **Clear** to delete logs manually as well.

4.1.11. Tools

The IEEE 802.11b/g/n VAP Access Points provide two tools to test the link status with other VAP-managed Access Points or anyone on the network.

Ping

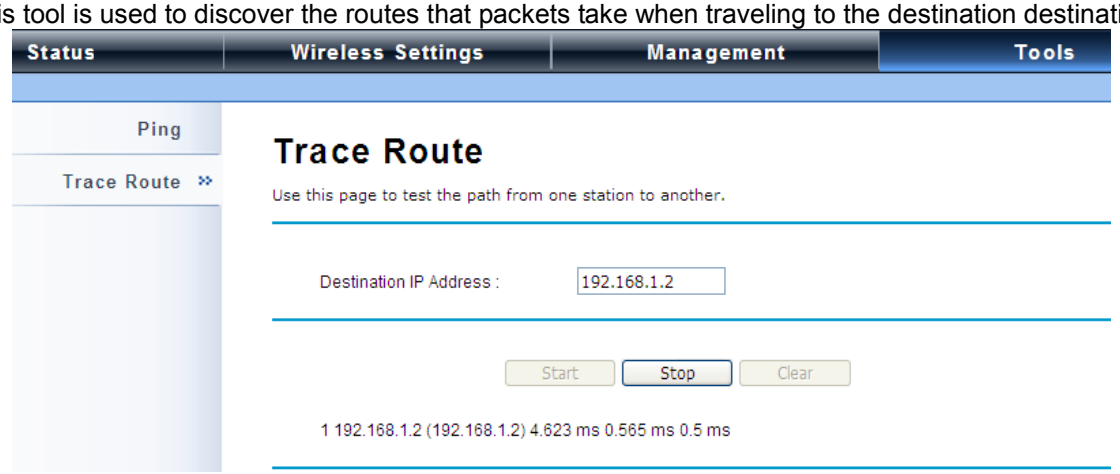
Ping Address
Enter IP address of the remote destination.

- **Ping Count:**
  Enter the number of pings.

- **Packet Size**:
  Specify ping packet size.

Trace Route

This tool is used to discover the routes that packets take when traveling to the destination destination.

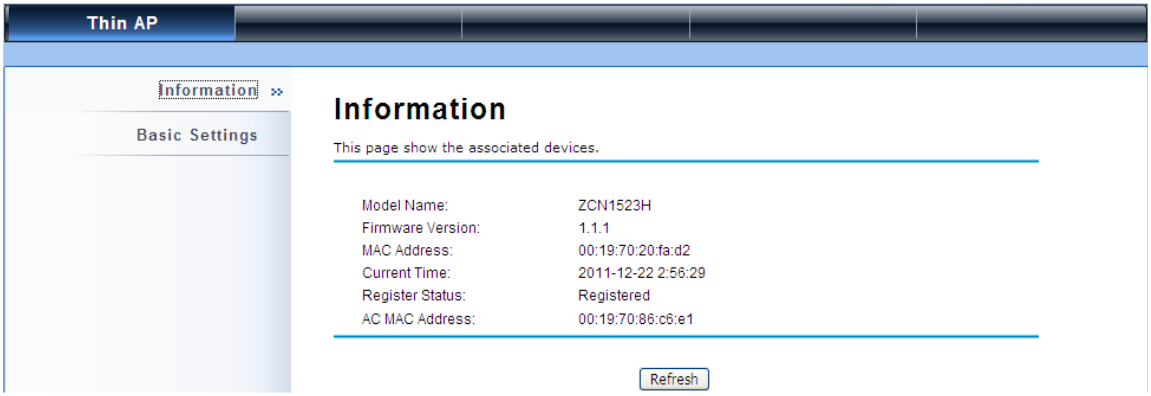


- **Destination IP Address**
  Enter IP address of the remote destination and click **Start** to start.

4.2. *Thin AP Mode*

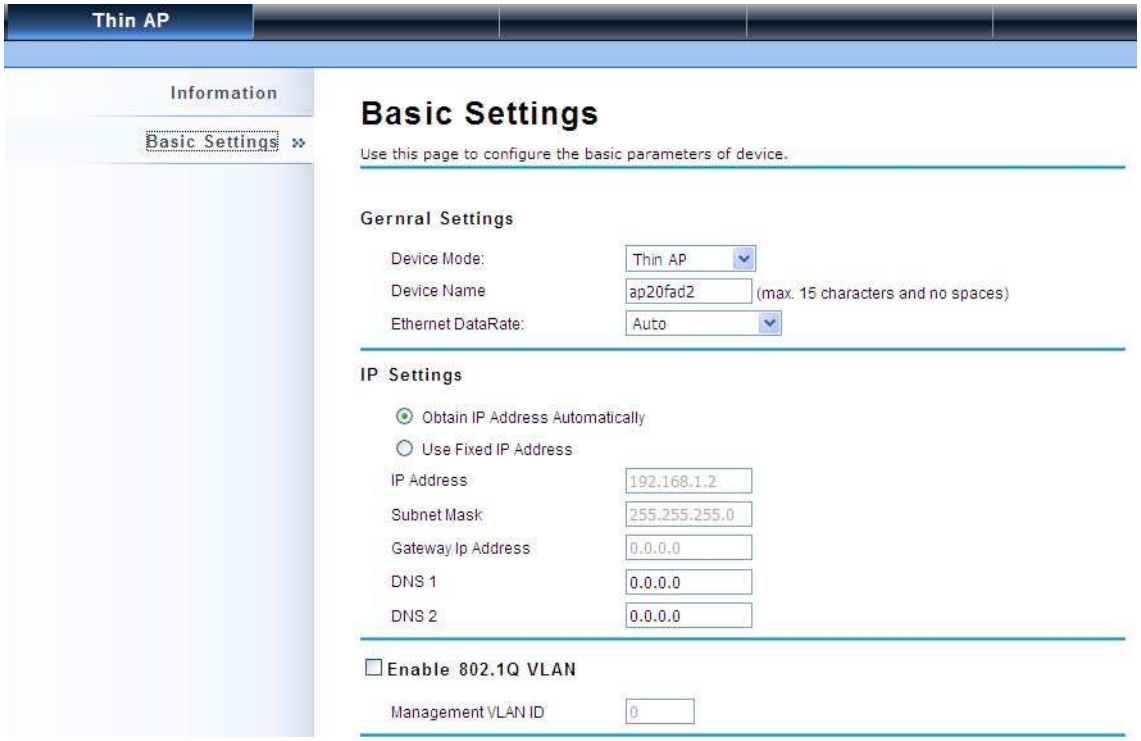
4.2.1. Information

You may see some VAP-managed AP's basic information such as model name, firmware version, MAC address, current up time, registration status as well as MAC address.



4.2.2. Basic Settings

Allows you to configure device and IP settings for the VAP-managed AP.



General Settings:

Device Mode: Three modes are provided: **AC+Thin AP**, **Thin AP**, **FAT AP**. Select AC+Thin AP to have the device act as virtual access controller to manage other VAP-managed APs on your network. Select "Thin AP" to have the VAP Access Point managed by the VAP AP in AC mode. Select FAT AP to perform as a standalone AP, neither managing nor managed by other VAP APs.

Device Name: Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).

Ethernet Data Rate: Specify the transmission rate of data for Ethernet. Default is **Auto**.

- **IP Address Assignment:**
  Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option, thus the VAP Access Pioint is able to obtain IP settings automatically from the DHCP server.

  Use Fixed IP Address: Check this option. You have to specify a static IP address, subnet mask, default gateway and DNS server for the VAP Access Point manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

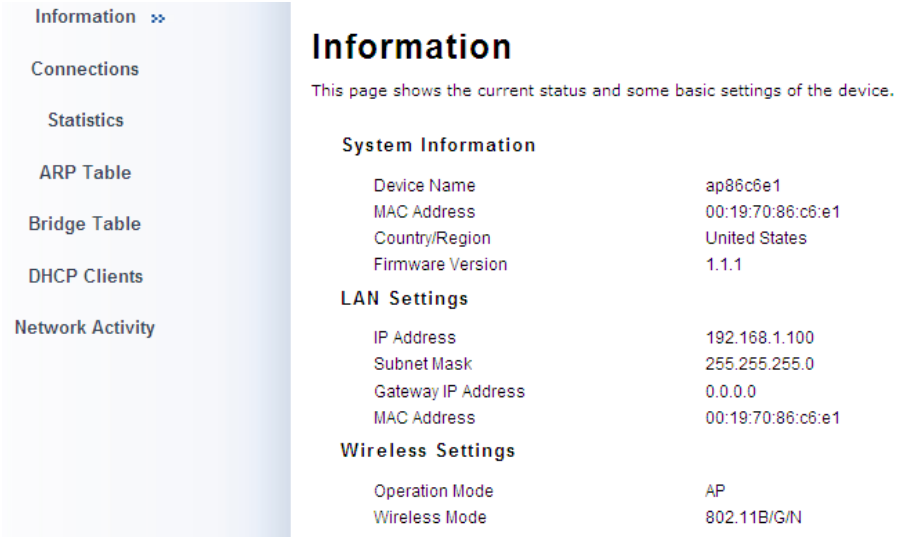
- **Enable 802.1Q VLAN**
  To be able to access the web page of the VAP-managed AP in the VLAN network, you need to assign the VLAN management ID for the VAP-managed AP. Note that the ID on the switch must be identical of the AP's VLAN ID. Check **Enable 802.1Q VLAN** checkbox to activate it.
  Management VLAN ID: Enter the VLAN ID.

4.3. *FAT AP Mode*

4.3.1. Status

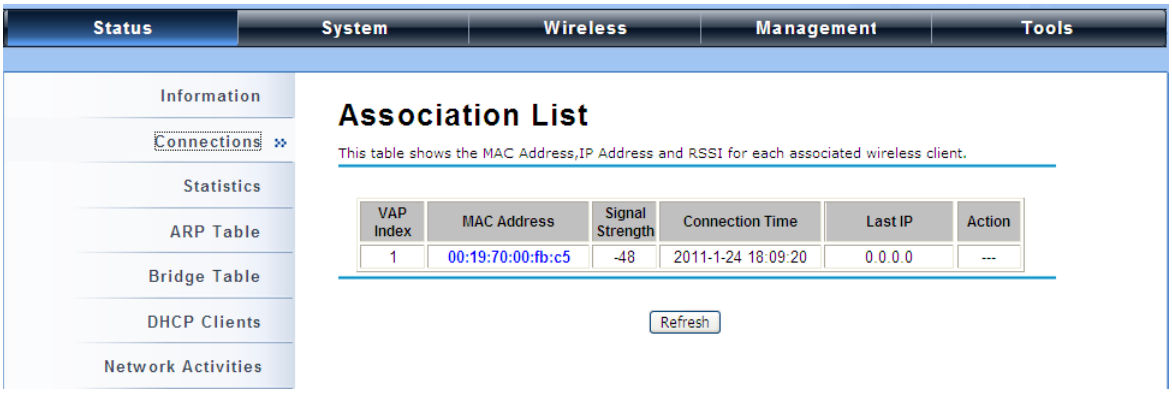
View Basic Information

Open "**Information**" in "**Status**" to check the basic information of the VAP Access Point, which is read only. Information includes system information, LAN settings, wireless setting and interface status. Click "**Refresh**" at the bottom to have the real-time information.

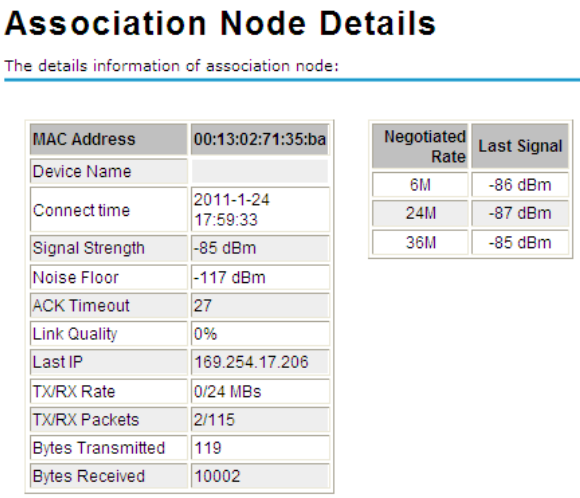


View Association List

Open "**Connections**" in "**Status**" to check the information of associated wireless devices such as MAC address, signal strength, connection time, IP address, etc. All is read only. Click "**Refresh**" at the bottom to update the current association list.

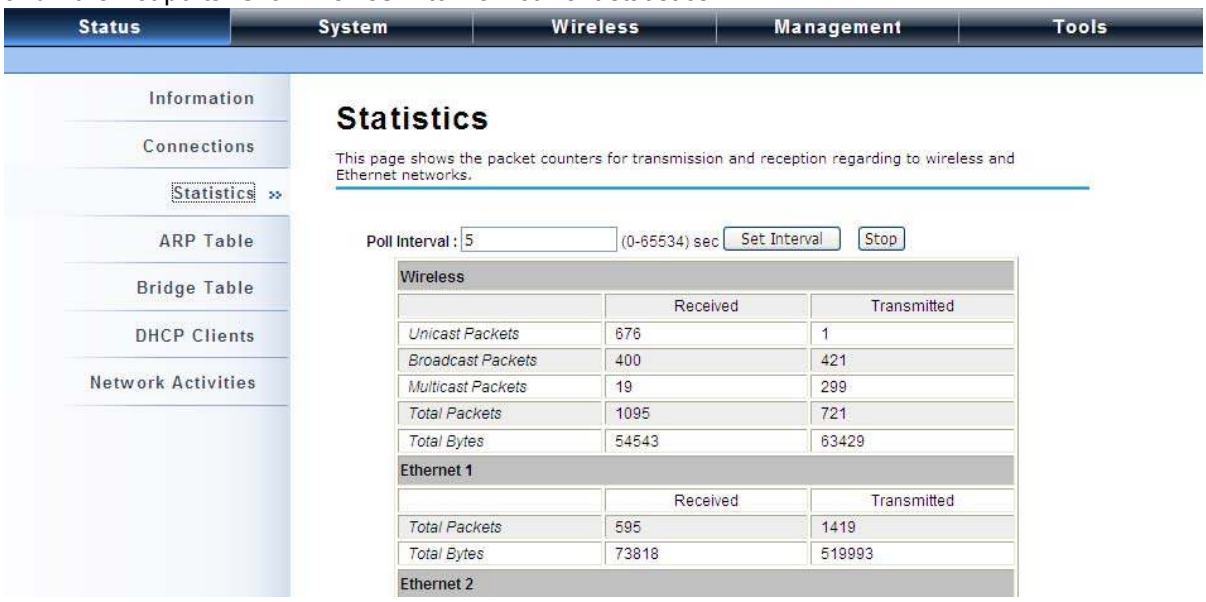


By clicking on the MAC address of the selected device on the web you may see more details including device name, connection time, signal strength, noise floor, ACK timeout, link quality, IP information, current data rate, current TX/RX packets.



View Network Flow Statistics

Open "**Statistics**" in "**Status**" to check the data packets received on and transmitted from the wireless and Ethernet ports. Click "**Refresh**" to view current statistics.

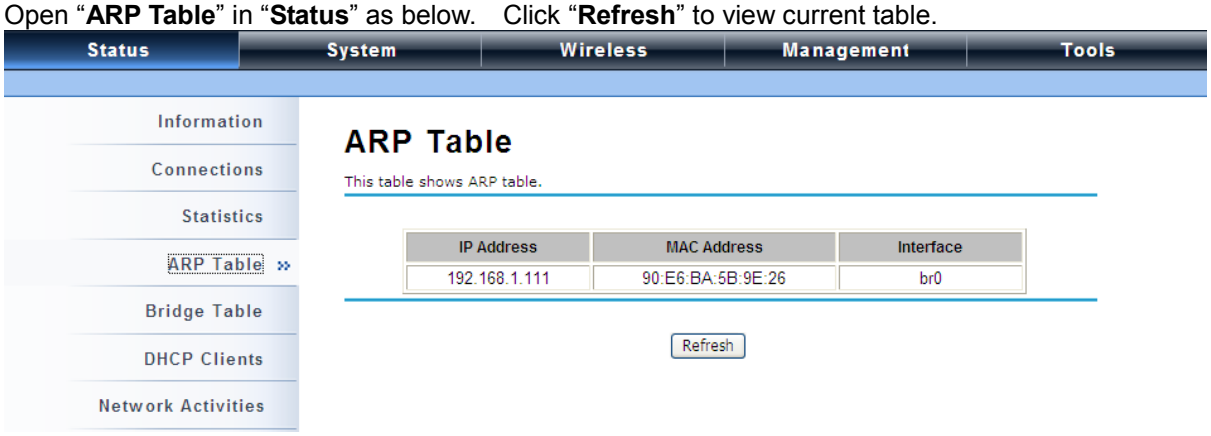


- **Poll Interval**
  Specify the refresh time interval in the box beside "**Poll Interval**" and click "**Set Interval**" to save

settings. “**Stop**” helps to stop the auto refresh of network flow statistics.

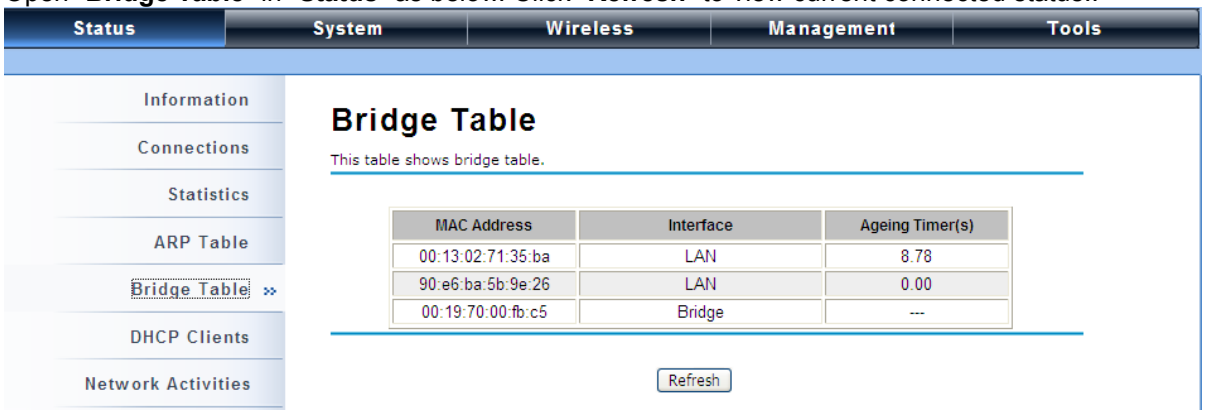
View ARP Table

Open “**ARP Table**” in “**Status**” as below. Click “**Refresh**” to view current table.



View Bridge Table

Open “**Bridge Table**” in “**Status**” as below. Click “**Refresh**” to view current connected status..

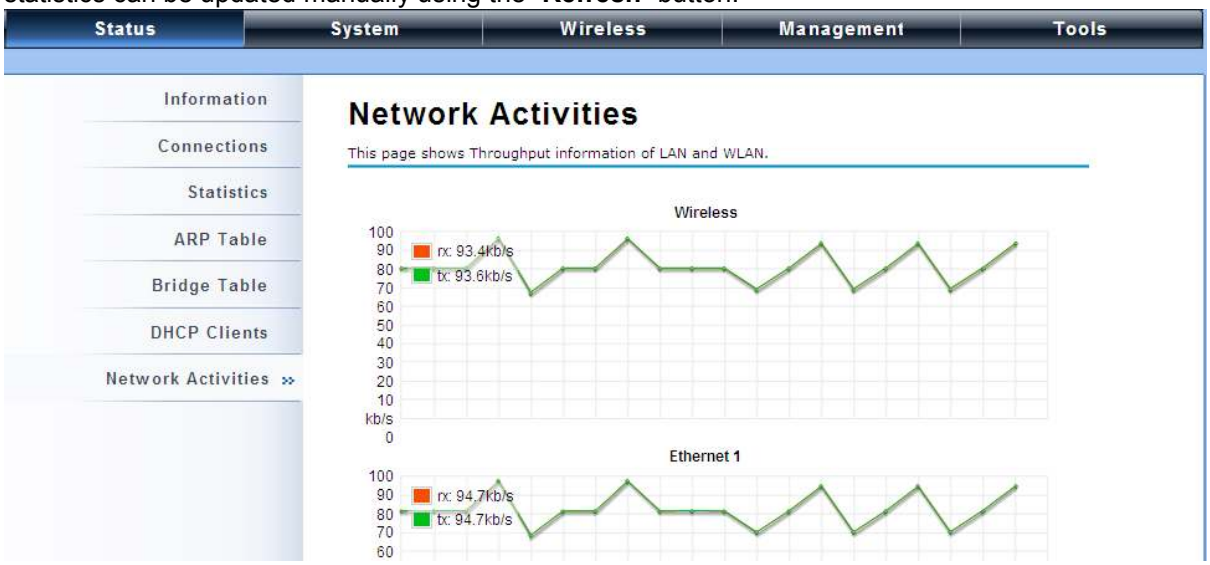


View Active DHCP Client Table

Open “**DHCP Clients**” in “**Status**” as below to check the assigned IP address, MAC address and time expired for each DHCP leased client. Click “**Refresh**” to view current table.

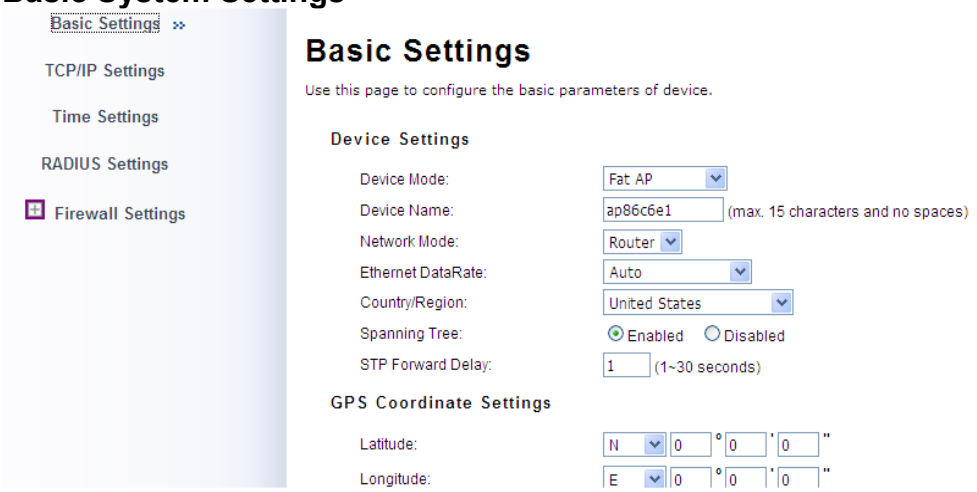
View Network Activities

The network activities allows you to monitor the current Wireless and Ethernet TX/RX data traffic in graphical and numerical form on the Web of the Skyport. The chart scale and throughput dimension (Bps, Kbps, Mbps) changes dynamically according to the mean throughput value. Throughput statistics can be updated manually using the "**Refresh**" button.



4.3.2. System

Basic System Settings


Basic Settings
TCP/IP Settings
Time Settings
RADIUS Settings
Firewall Settings
Basic Settings
Use this page to configure the basic parameters of device.
Device Settings
Device Mode: Fat AP
Device Name: ap86c6e1 (max. 15 characters and no spaces)
Network Mode: Router
Ethernet DataRate: Auto
Country/Region: United States
Spanning Tree: Enabled Disabled
STP Forward Delay: 1 (1~30 seconds)
GPS Coordinate Settings
Latitude: N 0 ° 0 ' 0 "
Longitude: E 0 ° 0 ' 0 "

- **Device Settings**

Device Mode: Three modes are provided: **AC+Thin AP**, **Thin AP**, **FAT AP**. Select AC+Thin AP to have the device act as virtual access controller to manage other VAP-managed APs on your network. Select "Thin AP" to have the VAP Access Point managed by the VAP AP in AC mode. Select FAT AP to perform as a standalone AP, neither managing nor managed by other VAP APs.

Device Name: Specify the device name, which is composed of no more than 15 characters with (0-9), (A-Z), (a-z) or (-).

Network Mode: Specify the network mode, including Bridge and Router. It is easy to configure parameters in Bridge Mode; however, users must pay extra attention to the way they configure the device when it is set to Router Mode. For details, please refer to **TCP/IP Settings"**.

Ethernet Data Rate: Specify the transmission rate of data for Ethernet. Default is **Auto**.

Country Region: The availability of some specific channels and/or operational frequency bands is country dependent.

Spanning Tree: Spanning Tree Protocol (STP) is a link management protocol for AP which provides path redundancy while preventing loops in a network. STP allows only one active path at a time between the access points but establish the redundant link as a backup if the initial link fails.

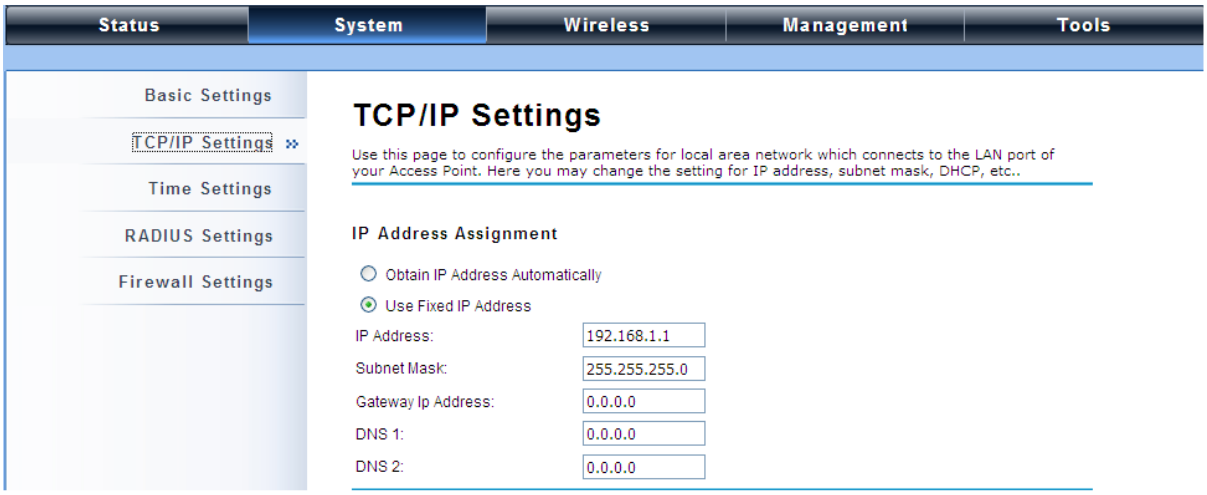
STP Forward Delay: STP Forward Delay is the time spent in detecting and learning network tree topology state before entering the forward state. Default time value is 1 sec.

- **GPS Coordinate Settings**

  The GPS Coordinate Setting helps you mark the latitude and longitude of the VAP Access Point. Just enter the coordinates and click the **Apply** button.

TCP/IP Settings

Open "**TCP/IP Settings**" in "**System**" as below to configure the parameters for LAN which connects to the LAN port of the VAP Access Point. In this page, users may change the settings for IP Address, Subnet Mask, and DHCP Server.



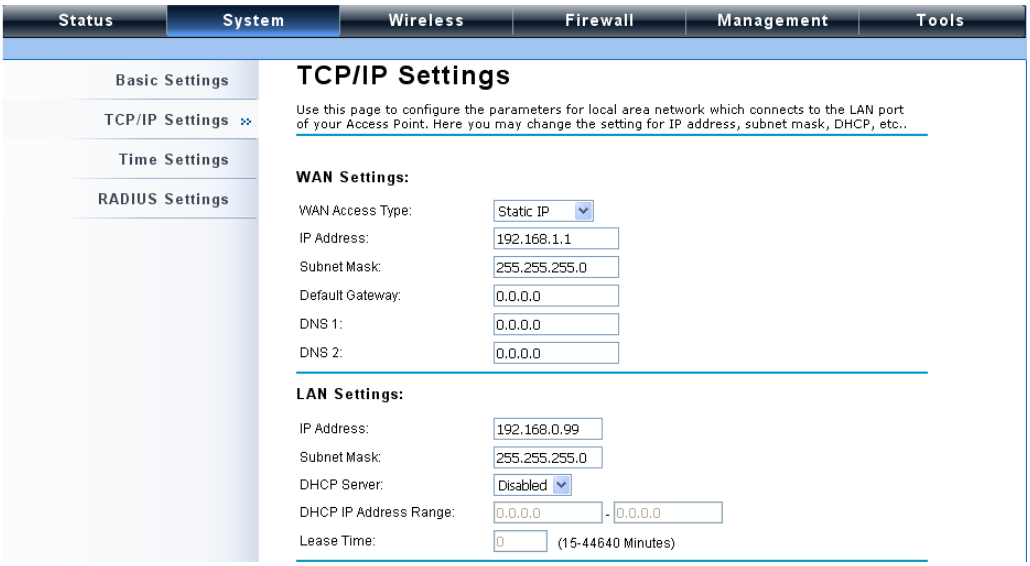
Obtain IP Address Automatically: If a DHCP server exists in your network, you can check this option, thus the VAP Access Point is able to obtain IP settings automatically from that DHCP server.

Note:

- When the IP address of the VAP Access Point is changed, the clients on the network often need to wait for a while or even reboot before they can access the new IP address. For an immediate access to the bridge, please flush the netbios cache on the client computer by running the "nbtstat –r" command before using the device name of the VAP Access Point to access its Web Management page.
- In case the VAP Access Point is unable to obtain an IP address from a valid DHCP server, it will fall back to default static IP address.

Use Fixed IP Address: Check this option. You have to specify a static IP address, subnet mask, default gateway and DNS server for the VAP ACCESS POINT manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict.

If the VAP Access Point is configured as Router mode, you need to configure some additional TCP/IP parameters for accessing the Internet.



WAN Settings: Specify the Internet access method to Static IP, DHCP or PPPOE. Users must enter WAN IP Address, Subnet Mask, Gateway settings provided by your ISPs.

LAN Settings: When DHCP Server is disabled, users can specify IP address and subnet mask for the VAP ACCESS POINT manually. Make sure the specified IP address is unique on your network in order to prevent IP conflict. When DHCP Server is enabled, users may specify DHCP IP Address Range, DHCP Subnet Mask, DHCP Gateway and Lease Time (15-44640 minutes). A DHCP relay agents is used to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. To enable the DHCP relay agent, check the "**Enable DHCP Relay**" checkbox and enter the IP address of the DHCP server.

Warning:

- In AP mode, the VAP Access Point must establish connection with another wireless device before it is set to Router mode. To access the unit in Router mode via wired port, please type the WAN IP address to enter the web page for WAN

is on wired port and LAN is on wireless port. Or, you can access device through the wireless device connected with the VAP AP.

- In wireless client mode, users can access the VAP Access Point via its wired port, for WAN is on wireless port and LAN is on wired port when device is set to Router mode.
- Bridge mode and AP Repeater mode are similar to AP mode when device is set to Router mode; WAN is on wired port and LAN is on wireless port. Thus users must also connect the VAP Access Point with another wireless device before it is set to Router mode and access the VAP Access Point via the connected wireless device.

Time Settings

Compliant with NTP, the VAP Access Point is capable of keeping its time in accord with the Internet time. To use this feature, check **Enable NTP Client Update** in advance.

- **Current Time**
  Display the present time in Yr, Mon, Day, Hr, Min and Sec.

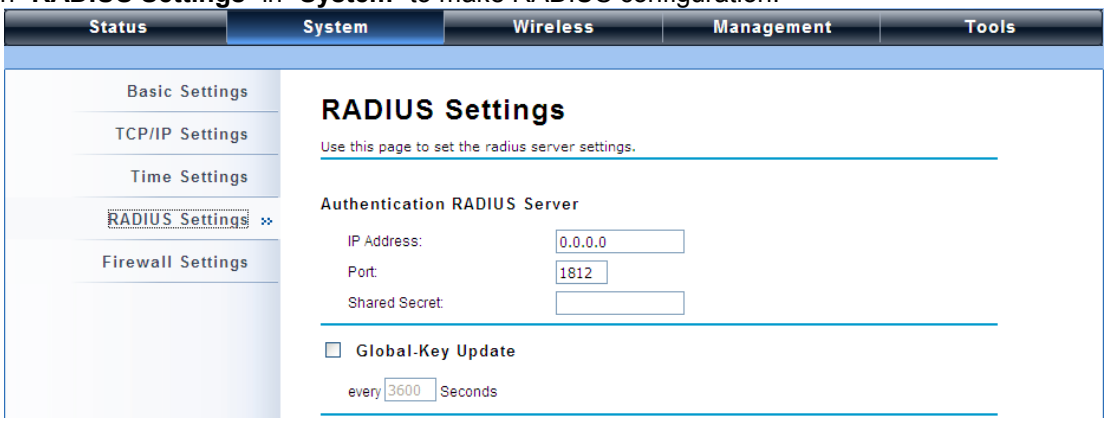
- **Time Zone Select**
  Select the time zone from the dropdown list.

- **NTP Server**
  Select the time server from the "**NTP Server**" dropdown list. or manually input the IP address of available time server into "**Manual IP**".

RADIUS Settings

RADIUS (Remote Authentication Dial-In User Service) is a server for remote user authentication and accounting; playing a central role in the network in providing the capabilities of authenticating, authorizing, accounting, auditing, alarming and etc. It allows an organization to maintain user profiles in a central database that all remote servers can share. If 802.1X, WPA(2) is used, you need to configure radius settings.

Open "**RADIUS Settings**" in "**System**" to make RADIUS configuration.



- **Authentication RADIUS Server**
  This is for RADIUS authentication. It can communicate with RADIUS through IP Address, Port and Shared Secret.

  IP Address: Enter the IP address of the Radius Server;

  Port: Enter the port number of the Radius Server;

  Shared Secret: This secret, which is composed of no more than 31 characters, is shared by the VAP Access Point and RADIUS during authentication.

- **Global-Key Update**
  Check this option and specify the time interval between two global-key updates. Default is 3600 seconds.

Firewall Settings

The firewall is a system or group of systems that enforce an access control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. The VAP Access Point has capabilities of Source IP Filtering, Destination IP Filtering, Source Port Filtering, Destination Port Filtering, Port Forwarding as well as DMZ. This is available only under **Router** Mode.

- **Source IP Filtering:**

You may create and activate a rule that filters a packet based on the source IP address from your local network to Internet. Check "Enable Source IP Filtering**" to activate rule.**

Local IP Address: Enter the IP address you would like to restrict.

Comment: Make comments to record your filtering rule.
Click **Apply** and the IP address will be added in the list. To delete the IP address from filtering, click **Select** checkbox of the designated IP address and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

- **Destination IP Filtering:**

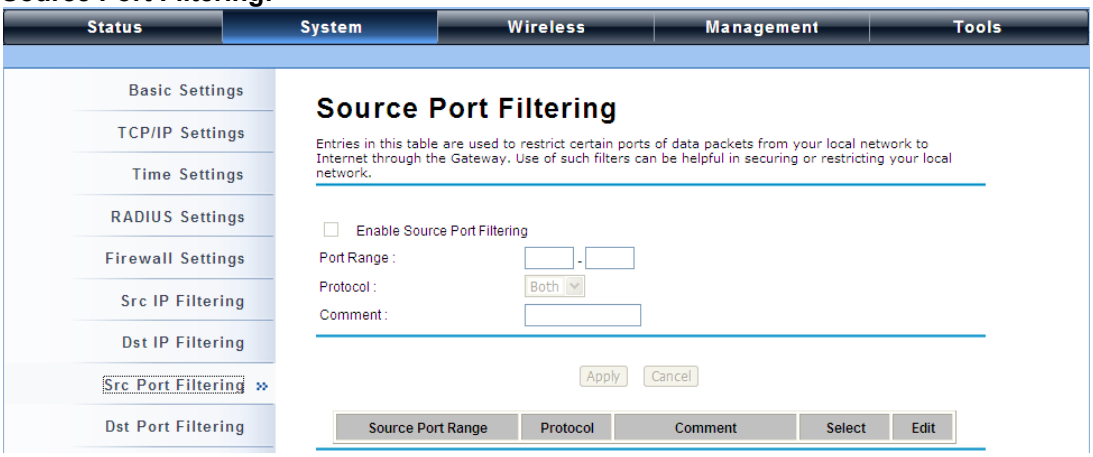
You may create and activate a rule that filters a packet based on the destination IP address to restrict the local computers from accessing certain websites. Check "**Enable Destination IP Filtering**" to activate rule.

Destination IP Address: Enter the IP address to be restricted.

Comment: Make comments to record your filtering rule.

Click **Apply** and the IP address will be added in the list. To delete the IP address from filtering, click **Select** checkbox of the designated destination IP address and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

- **Source Port Filtering:**



You may create and activate a rule that filters a packet based on the source port from your local network to Internet. Check "**Enable Source Port Filtering**" to activate rule.

Port Range: Enter the port range you would like to restrict.

Protocol: Select port protocol: **Both**, **TCP**, **UDP**.

Comment: Make comments to record your filtering rule.

Click **Apply** and the IP address will be added in the list. To delete the restricted source ports, click **Select** checkbox of the designated ports and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**

- **Destination Port Filtering:**

You may create and activate a rule that filters a packet based on the destination port from your local network to Internet. Check "**Enable Destination Port Filtering**" to activate rule.

Port Range: Enter the port range you would like to restrict.

Protocol: Select port protocol: **Both**, **TCP**, **UDP**.

Comment: Make comments to record your filtering rule.
Click **Apply** and the IP address will be added in the list. To delete the restricted destination ports, click **Select** checkbox of the designated ports and click the **Delete Selected** button. You may delete all the IP addresses in the list by clicking **Delete All**.

- **Port Forwarding:**

The port forwarding allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings ne are only necessary if you wish to host some sort of server like a web server or mail server on the private local network VAP Access Point's NAT firewall. Check the **Enable Port Forwarding** checkbox to activate port forwarding.

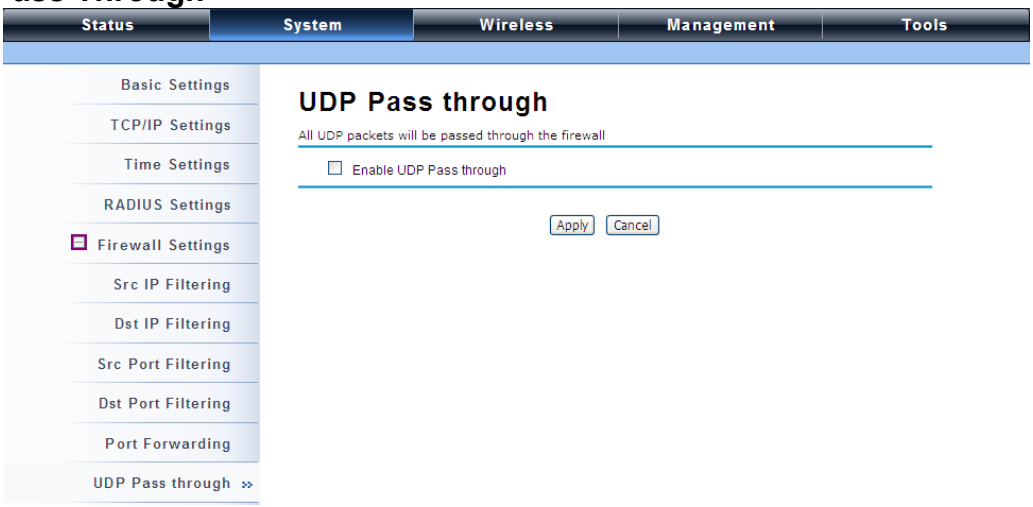
IP Address: Enter the IP address the local server.

Protocol: Select **Both**, **UDP** or **TCP**.

Port Range: Specify the port range.

Comment: Make comments to record the port forwarding rule.

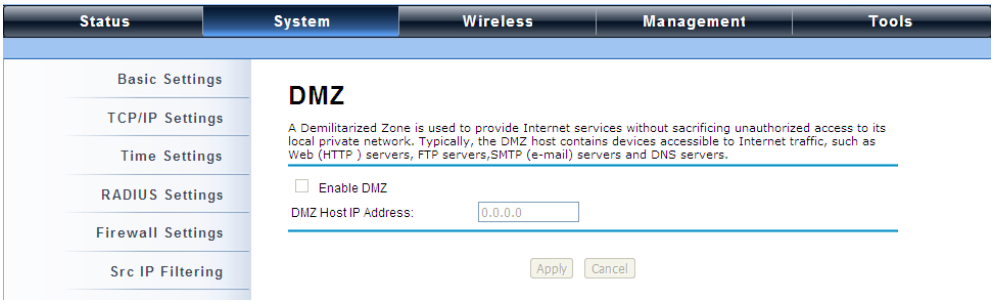
UDP Pass Through



By check **Enable UDP Pass through** will allow all the UDPs packets to pass through the firewall. Note that opening all the UDP ports will be very likely to expose the network to intruders

DMZ:

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to the Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. To activate DMZ, check the **Enable DMZ** checkbox.



DMZ Host IP Address: Enter the local host IP address.

4.3.3. Wireless

Open “**Basic Settings**” in “**Wireless**” as below to make basic wireless configuration.

- **Disable Wireless LAN Interface**

  Check this option to disable WLAN interface, then the wireless module of VAP Access Point will stop working and no wireless device can connect to it.

- **Operation Mode**

  Four operating modes are available in VAP Access Point when acts as a FAT AP.

  AP: The VAP Access Point establishes a wireless coverage and receives connectivity from other wireless devices.

  Wireless Client: The VAP Access Point is able to connect to the AP and thus join the wireless network around it.

  Bridge: The VAP Access Point establishes wireless connectivity with other APs by keying in remote MAC address. Please refer to the “**WDS Settings**” for detailed configuration.

  AP Repeater: The VAP Access Point servers as AP and Bridge concurrently. In other words, the VAP Access Point can provide connectivity services for CPEs under Bridge mode.

Wireless Network Name (SSID)

This wireless network name is shared among all associated devices in your wireless network. Keep it identical on all those devices. Note that the SSID is case-sensitive and can not exceed 32 characters.

- **Broadcast SSID**

  Under AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA can not scan and find VAP Access Point, so that malicious attack by some illegal STA could be avoided.

- **802.11 Mode**

  The VAP Access Point can communicate with wireless devices of 802.11b/g or 802.11b/g/n.

- **HT Protect**

  Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the

one with HT protect enabled gets higher throughput.

- **Frequency/Channel**
  Channel varies much as the available band differs from country to country. Select a proper operating channel in the drop-down list according to your situation.

- **Extension Channel**
  Only applicable to AP, AP Repeater, and 40MHz channel width) indicates the use of channel bonding that allows the VAP Access Point to use two channels at once. Two options are available: Upper Channel and Lower Channel.

- **Channel Mode**
  Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.

- **Antenna**
  By default, VAP Access Point uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from “Internal (8 dBi)” to”External (N-Type)”.

  When **External (N-Type)** is selected, an Antenna Gain bar will appear to allow you specify the

gain of the external antenna. The antenna gain calculates the TX power back off needed to remain in compliance with regulations.

Note:

- You are able to choose “External (N-Type)” only when you have well done installing the external antenna; otherwise, it might damage VAP Access Point itself.
- The maximum output power will vary depending on the country selected in order to comply with the local regulation.
- The output power here is counted from the RF single chain only not including the 8dBi internal antenna.

- **Maximum Output Power (per chain):**

  Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly. The output power will vary depending on each country’s regulation.

- **Data Rate**

  Usually “**Auto**” is preferred. Under this rate, the VAP Access Point will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

- **Extension Channel Protection Mode**

  This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

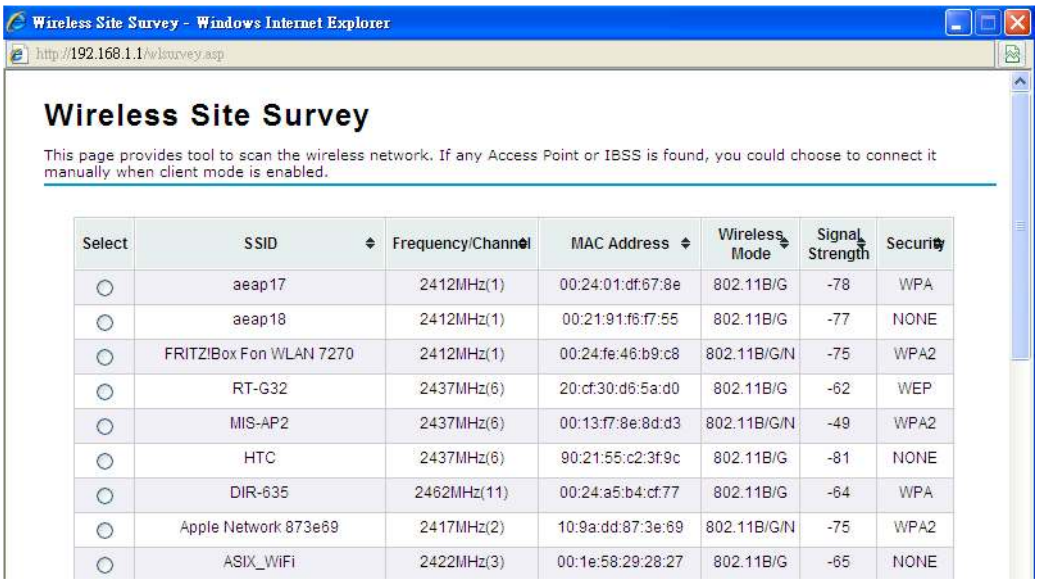
- **Enable MAC Clone**

  Available only under wireless client mode, it hides the MAC address of the AP while displays the one of associated wireless client or the MAC address designated manually.

- **Site Survey**

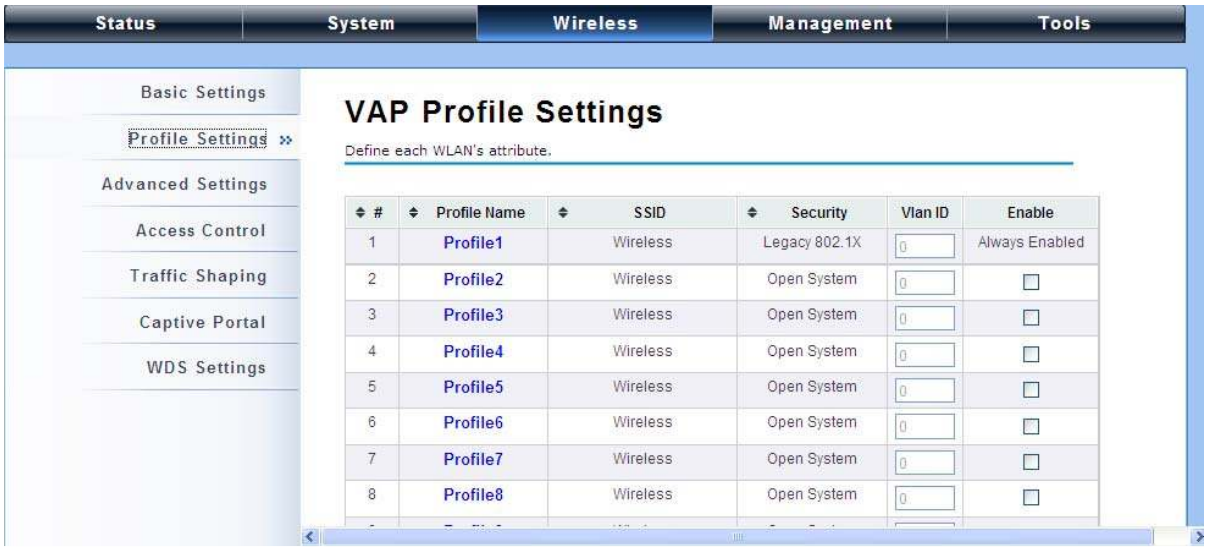
  Under wireless client mode, the VAP Access Point is able to perform site survey, through which, information on the available access points will be detected.

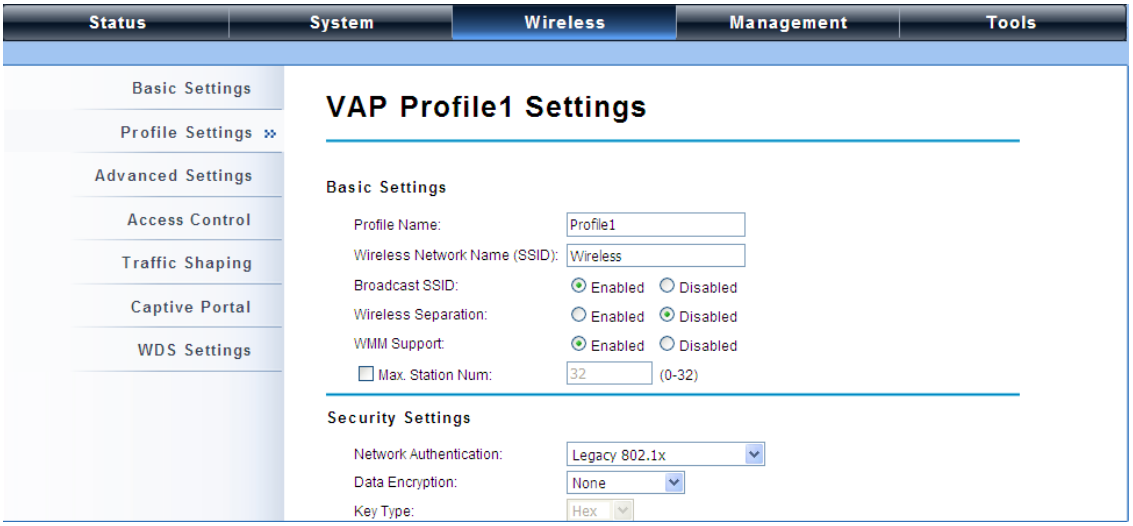
Open “**Basic Settings**” in “**Wireless**”, by clicking the “**Site Survey**” button beside “**Wireless Mode**” option, the wireless site survey window will pop up with a list of available AP in the vicinity. Select the AP you would like to connect and click “**Selected**” to establish connection.


Wireless Site Survey - Windows Internet Explorer
http://192.168.1.1/wlsurvey.asp
Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
Select
SSID
Frequency/Channel
MAC Address
Wireless Mode
Signal Strength
Security
aeap17 2412MHz(1) 00:24:01:df:67:8e 802.11B/G -78 WPA
aeap18 2412MHz(1) 00:21:91:f6:f7:55 802.11B/G -77 NONE
FRITZ!Box Fon WLAN 7270 2412MHz(1) 00:24:fe:46:b9:c8 802.11B/G/N -75 WPA2
RT-G32 2437MHz(6) 20:cf:30:d6:5a:d0 802.11B/G -62 WEP
MIS-AP2 2437MHz(6) 00:13:f7:8e:8d:d3 802.11B/G/N -49 WPA2
HTC 2437MHz(6) 90:21:55:c2:3f:9c 802.11B/G -81 NONE
DIR-635 2462MHz(11) 00:24:a5:b4:cf:77 802.11B/G -64 WPA
Apple Network 873e69 2417MHz(2) 10:9a:dd:87:3e:69 802.11B/G/N -75 WPA2
ASIX_WiFi 2422MHz(3) 00:1e:58:29:28:27 802.11B/G -65 NONE

VAP Profile Settings

Available in AP mode, the VAP Access Point allows up to 16 virtual SSIDs on a single BSSID and to configure different profile settings such as security and VLAN ID to each SSID. To create a virtual AP, you may check the **Enable** box of the profile and click on the profile (eg. Profile 2) to configure wireless and security settings. Hit **Apply** to active the profile.





- **Basic Setting**

Profile Name: Name of the VAP profile

Wireless Network Name: Enter the virtual SSID for the VAP

Broadcast SSID: In AP mode, hiding network name is necessary when you are in a wireless environment that may have potential risk. By disabling broadcast SSID, the STA cannot scan and find the VAP Access Point, so that malicious attack by some illegal STA could be avoided.

Wireless Separation: Wireless separation is an ideal way to enhance the security of network transmission. Under the mode except wireless client mode, enable "**Wireless Separation**" can prevent the communication among associated wireless clients.

WMM Support: WMM (Wi-Fi Multimedia) is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type under AP mode only, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should also support it

Max. Station Number: By checking the "**Max. Station Num**" the VAP Access Point will only allow up to 32 wireless clients to associate with for better bandwidth for each client. By disabling the checkbox the VAP Access Point will allow up to 128 clients to connect, but it is likely to cause network congestion or poor performance.

- **Security Setting:**
To prevent unauthorized radios from accessing data transmitting over the connectivity, the IEEE 802.11a/n VAP Access Point provides you with rock solid security settings.

- **Network Authentication**

Open System: It allows any device to join the network without performing any security check.

Shared Key: Data encryption and key are required for wireless authentication (Not available in Bridge/AP Repeater mode).

Legacy 802.1x: It provides the rights to access the wireless network and wired Ethernet. With User and PC identity, centralized authentication as well as dynamic key management, it controls the security risk of wireless network to the lowest. To serve the 802.1x, at least one EAP type should be supported by the RADIUS Server, AP and wireless client.

WPA with RADIUS: Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard.

With warrant (username, password and etc.) offered by user, this kind of authentication can be realized with specific RADIUS server. This is the common way to be adopted in large enterprise network.

WPA2 with RADIUS: WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. If it is selected, AES encryption and RADIUS server are required.

WPA&WPA2 with RADIUS: It provides options of WPA (TKIP) or WPA2 (AES) for the client. If it is selected, the data encryption type must be TKIP + AES and the RADIUS server must be set.

Note:

- If Radius relevant authentication type is selected, please go to **Wireless** □ **Radius Settings** for further radius server configuration.

WPA-PSK: It is a simplified WPA mode with no need for specific authentication server. In this so-called WPA Pre-Shared Key, all you have to do is just pre-enter a key in each WLAN node and this is the common way to be adopted in large and middle enterprise as well as residential network.

WPA2-PSK: As a new version of WPA, only all the clients support WPA2, can it be available. If it is selected, the data encryption can only be AES and the passphrase is required.

WPA-PSK&WPA2-PSK: Available in AP mode, it provides options of WPA (TKIP) or WPA2 (AES)

encryption for the client. If it is selected, the data encryption can only be TKIP + AES and the passphrase is required.

- **Data Encryption**
  If data encryption is enabled, the key is required and only sharing the same key with other wireless devices can the communication be established.

  None: Available only when the authentication type is open system.

  64 bits WEP: It is made up of 10 hexadecimal numbers.

  128 bits WEP: It is made up of 26 hexadecimal numbers.

  152 bits WEP: It is made up of 32 hexadecimal numbers.

  TKIP: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK, etc.

  AES: Advanced Encryption Standard, it is usually co-used with WPA2-PSK, WPA, WPA2, etc.

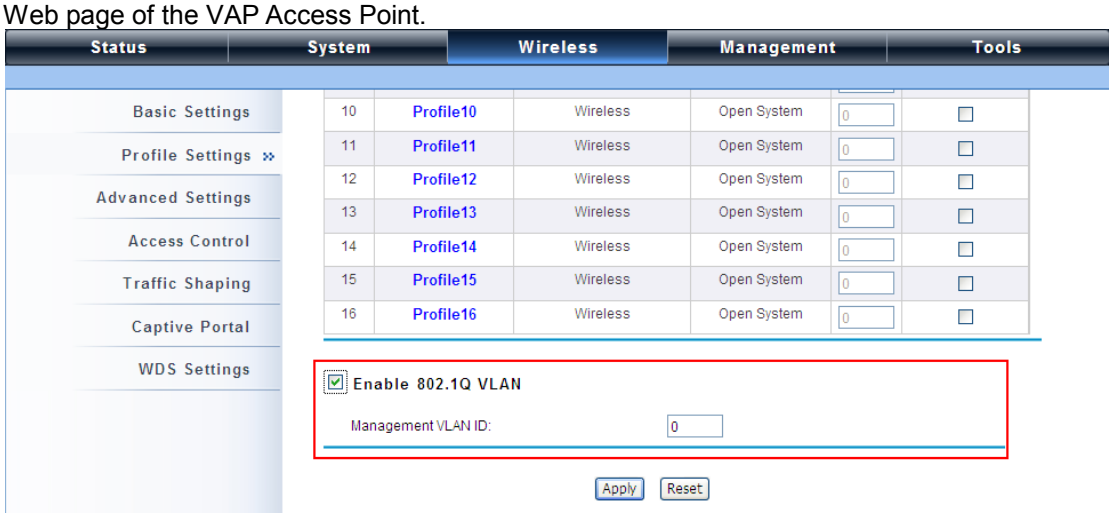
  TKIP + AES: It allows for backwards compatibility with devices using TKIP.

Note:

- We strongly recommend you enable wireless security on your network!
- Only the same Authentication, Data Encryption and Key among the IEEE 802.11b/g/n VAP Access Point and wireless clients can the communication be established!

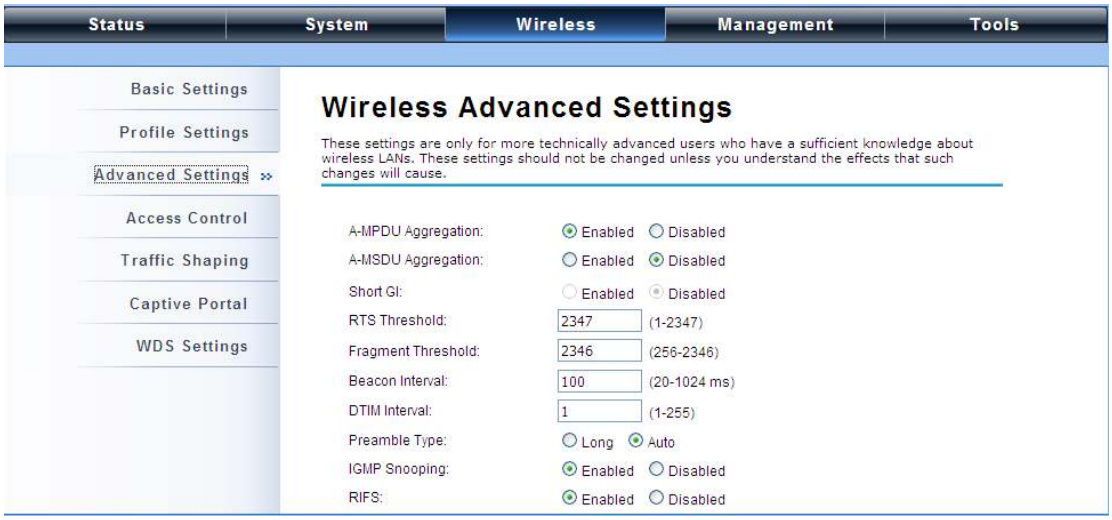
VLAN

If your network uses VLANs, you can assign one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN.
To allow users on the VLAN to access the WEB page of the IEEE 802.11a/n VAP Access Point, you need to enable "**Enable 802.1Q VLAN**" and assign a management VLAN ID for your device. Make sure the assigned management VLAN ID is identical to your network VLAN ID to avoid failures of accessing the Web page of the VAP Access Point.



Advanced Settings

Open "**Advanced Settings**" in "**Wireless**" to make advanced wireless settings.


Status
System
Wireless
Management
Tools
Basic Settings
Profile Settings
Advanced Settings
Access Control
Traffic Shaping
Captive Portal
WDS Settings
Wireless Advanced Settings
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LANs. These settings should not be changed unless you understand the effects that such changes will cause.
A-MPDU Aggregation: Enabled Disabled
A-MSDU Aggregation: Enabled Disabled
Short GI: Enabled Disabled
RTS Threshold: 2347 (1-2347)
Fragment Threshold: 2346 (256-2346)
Beacon Interval: 100 (20-1024 ms)
DTIM Interval: 1 (1-255)
Preamble Type: Long Auto
IGMP Snooping: Enabled Disabled
RIFS: Enabled Disabled

- **A-MPDU/A-MSDU Aggregation**

  The data rate of your AP except wireless client mode could be enhanced greatly with this option enabled; however, if your wireless clients don't support A-MPDU/A-MSDU aggregation, it is not recommended to enable it.

- **Short GI**

  Under 802.11n mode, enable it to obtain better data rate if there is no negative compatibility issue.

- **RTS Threshold**

  The VAP Access Point sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in byte. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Fragmentation Length**

  Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Beacon Interval**

  Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024.

- **DTIM Interval**

  DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.

- **Preamble Type**

  It defines some details on the 802.11 physical layer. "**Long**" and "**Auto**" are available.

- **IGMP Snooping**

  Available in AP/Router mode, IGMP snooping is the process of listening to IGMP network traffic. By enabling IGMP snooping, the AP will listen to IGMP membership reports, queries and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.

- **RIFS**

  RIFS (Reduced Interframe Spacing) is a means of reducing overhead and thereby increasing network efficiency.

- **Link Integration**

  Available under AP/Bridge/AP repeater mode, it monitors the connection on the Ethernet port by checking "**Enabled**". It can inform the associating wireless clients as soon as the disconnection occurs.

- **TDM Coordination**

  Stands for "Time-Division Multiplexing Technique", this resource reservation control mechanisms can avoid packet collisions and send the packets much more efficiently allowing for higher effective throughput rates. This function is only available in AP/CPE mode. It is highly recommended to enable TDM coordination when there are multiple CPEs needed to connect to the AP in your application.

- **LAN2LAN CPE**

  LAN2LAN CPE mode enables packet forwarding at layer 2 level. It is fully transparent for all the Layer2 protocols.

- **Space in Meter**

  To decrease the chances of data retransmission at long distance, the VAP Access Point can automatically adjust proper ACK timeout value by specifying distance of the two nodes.

- **Flow Control**

  It allows the administrator to specify the incoming and outgoing traffic limit by checking "**Enable Traffic Shaping**". This is only available in Router mode.

Note:

- We strongly recommend you leave most advanced settings at their defaults except “Distance in Meters” adjusted the parameter for real distance; any modification on them may negatively impact the performance of your wireless network.

Access Control

The Access Control appoints the authority to wireless client on accessing VAP Access Point, thus a further security mechanism is provided. This function is available only under AP/Router mode.
Open “**Access Control**” in “**Wireless Settings**” as below.

- **Profile Selection:** Select the VAP network you would like to enable access control.

- **Access Control Mode**
  If you select "**Allow Listed**", only those clients whose wireless MAC addresses are in the access control list will be able to connect to your AP. While when "**Deny Listed**" is selected, those wireless clients on the list will not be able to connect the AP.

- **MAC Address**
  Enter the MAC address of the wireless client that you would like to list into the access control list, click "**Apply**" then it will be added into the table at the bottom.

- **Delete Selected/All**
  Check the box before one or more MAC addresses of wireless client(s) that you would like to cancel, and click "**Delete Selected**" or "**Delete All**" to cancel that access control rule.

Traffic Shaping

It allows the administrator to manage the traffic flow to ensure optimal performance.

- **Overall Traffic Shaping**
  Check this box to control the overall bandwidth of the VAP Access Point.

  Incoming Traffic Limit: To specify maximum incoming bandwidth to a certain rate in kbit/s.

  Incoming Traffic Burst: To specify the buffer size for incoming traffic that can be sent within a given unit of time. The suggested value is 20KBytes. You may just leave the default value there, and then the connection will be bound to the traffic shaping rule at all times. You may decrease it to smaller value if the incoming traffic limit is smaller.

  Outgoing Traffic Limit: To limit the outbound traffic to a certain rate in kbit/s.

  Outgoing Traffic Burst: To specify the buffer size for outbound traffic. The suggested value is 20KBytes. You may decrease it to smaller value if the outbound traffic limit is smaller.

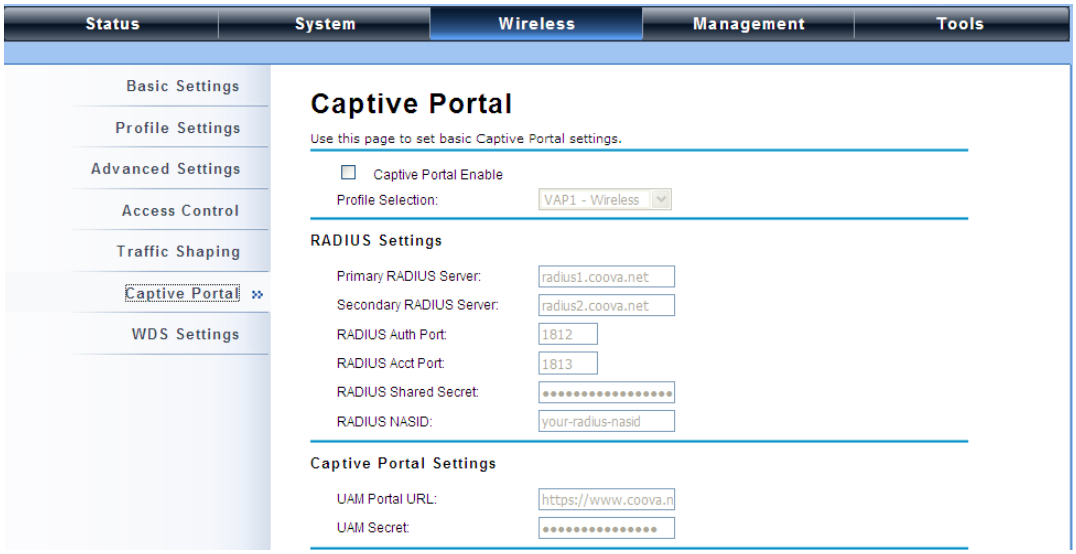
- **VAP Traffic Shaping**
  Check this box to control the overall bandwidth for a specific VAP network.

  Incoming Traffic Limit: To specify maximum incoming bandwidth to a certain rate in kbit/s.

  Incoming Traffic Burst: To specify the buffer size for incoming traffic that can be sent within a given unit of time. The suggested value is 20KBytes. You may just leave the default value there, and then the connection will be bound to the traffic shaping rule at all times. You may decrease it to smaller value if the incoming traffic limit is smaller.

Captive Portal

Captive portal is a management which allows WLAN users to easily and securely access the Internet. Under Router mode, when captive portal is enabled, the VAP Access Point will redirect the client to go to an authentication web page before browsing Internet web pages. Captive portals are used on most Wi-Fi hotspots networks. Therefore, to use captive portal, you need to find the service providers that have the additional services needed to make captive portal work.



To enable Captive Portal, check "**Captive Portal**" and select the VAP network needed for captive portal.

- **Radius Settings**
  Primary Radius Server: Enter the name or IP address of the primary radius server

  Secondary Radius Server: Enter the name or IP address of the primary radius server if any.

  Radius Auth Port: Enter the port number for authentication

  Radius Acct Port: Enter the port number for billing

  Radius Shared Secret: Enter the secret key of the radius server

  Radius NAS ID: Enter the name of the radius server if any

- **Radius Administrative-User:**
  Radius Admin Username: Enter the username of the Radius Administrator

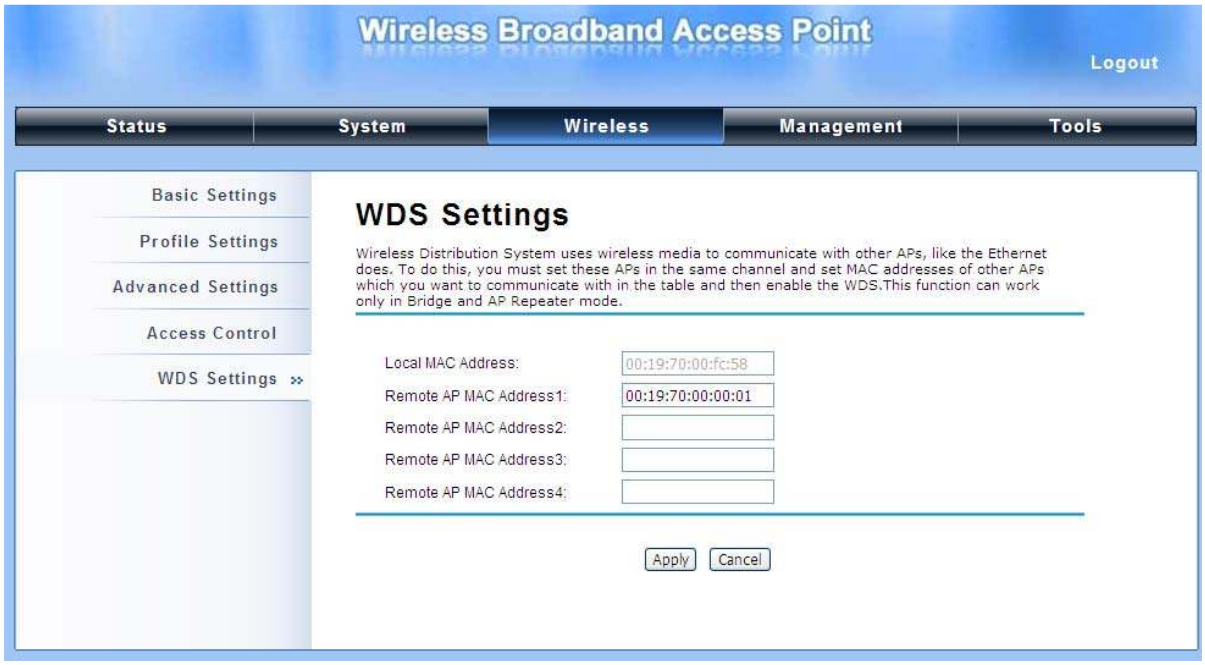
  Radius Admin Password: Enter the password of the Radius Administrator

- **Captive Portal**
  UAM Portal URL: Enter the address of the UAM portal server

  UAM Secret: Enter the secret password between the redirect URL and the Hotspot.

WDS Settings

Extend the range of your network without having to use cables to link the Access Points by using the Wireless Distribution System (WDS): Simply put, you can link the Access Points wirelessly. Open "**WDS Settings**" in "**Wireless**" as below


Wireless Broadband Access Point
Logout
Status
System
Wireless
Management
Tools
Basic Settings
Profile Settings
Advanced Settings
Access Control
WDS Settings
WDS Settings
Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC addresses of other APs which you want to communicate with in the table and then enable the WDS.This function can work only in Bridge and AP Repeater mode.
Local MAC Address:
00:19:70:00:fc:58
Remote AP MAC Address1:
00:19:70:00:00:01
Remote AP MAC Address2:
Remote AP MAC Address3:
Remote AP MAC Address4:
Apply
Cancel

Enter the MAC address of another AP you wirelessly want to connect to into the appropriate field and click "**Apply**" to save settings.

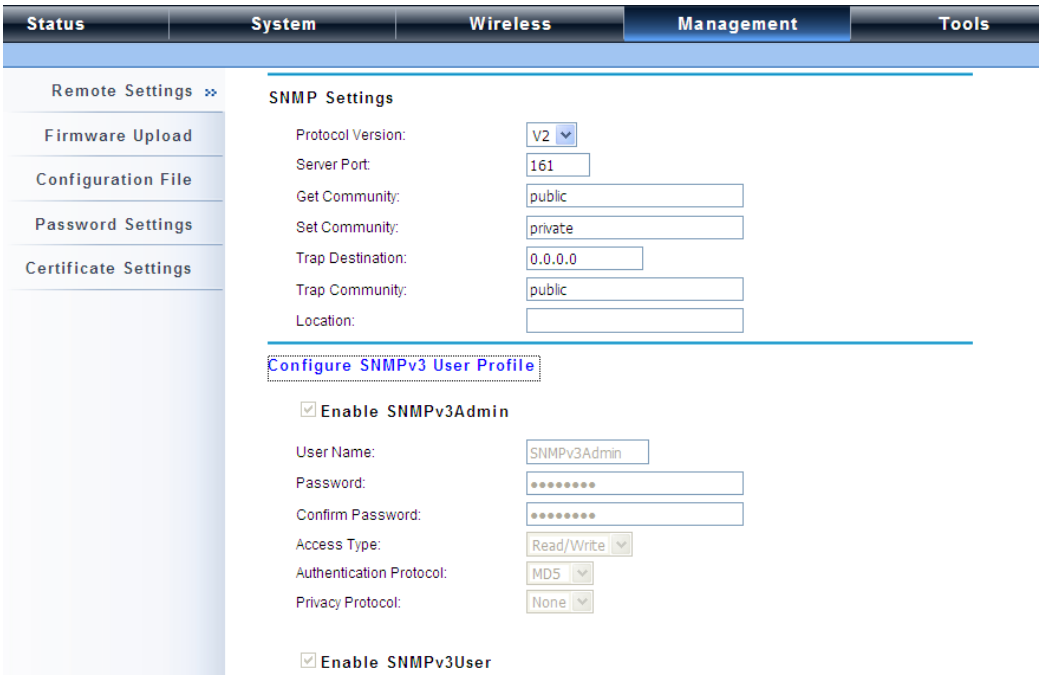
Note:

- WDS Settings is available only under Bridge and AP Repeater Mode.
- Bridge uses the WDS protocol that is not defined as the standard thus compatibility issues between equipment from different vendors may arise. Moreover, Tree or Star shape network topology should be used in all WDS use-cases (i.e. if AP2 and AP3 are specified as the WDS peers of AP1, AP2 should not be specified as the WDS peer of AP3 and AP3 should not be specified as the WDS peer of AP2 in any case). Mesh and Ring network topologies are not supported by WDS and should be avoided in all the use cases.

4.3.4. Remote Management

The VAP Access Point provides a variety of remotes managements including Telnet, SNMP, FTP, SSH, HTTPS and exclusive WISE tool, making configuration more convenient and secure.
With **Normal** selected, Telnet, SNMP and FTP are activated as default remote management options. To use secure management tools such as SSH, HTTPS and WISE, please select "**Secure**". You may also choose "**Customized**" to enable any methods as desired.

- **SNMP Management**
  The VAP Access Point supports SNMP for convenient remote management. Open "**Remote Settings**" in "**Management**" shown below. Set the SNMP parameters and obtain MIB file before remote management.



Protocol Version: Select the SNMP version, and keep it identical on the VAP Access Point and the SNMP manager. The VAP Access Point supports SNMP v2/v3.

Server Port: Change the server port for a service if needed; however you have to use the same port to use that service for remote management.

Get Community: Specify the password for the incoming Get and GetNext requests from the management station. By default, it is set to public and allows all requests.

Set Community: Specify the password for the incoming Set requests from the management station. By default, it is set to private.

Trap Destination: Specify the IP address of the station to send the SNMP traps to.

Trap Community: Specify the password sent with each trap to the manager. By default, it is set to public and allows all requests.

- **Configure SNMPv3 User Profile**

For SNMP protocol version 3, you can click "**Configure SNMPv3 User Profile**" in blue to set the details of SNMPv3 user. Check "**Enable SNMPv3 Admin/User**" in advance and make further configuration.

User Name: Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the VAP Access Point.

Password: Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access the IEEE 802.11b/g/n Wireless VAP Access Point.

Confirm Password: Input that password again to make sure it is your desired one.

Access Type: Select "**Read Only**" or "**Read and Write**" accordingly.

Authentication Protocol: Select an authentication algorithm. SHA authentication is stronger than MD5 but is slower.

Privacy Protocol: Specify the encryption method for SNMP communication. None and DES are available. **None** means no encryption is applied. **DES** is a Data Encryption Standard that

applies a 58-bit key to each 64-bit block of data.

Upgrade Firmware

Open “**Firmware Upload**” in “**Management**” and follow the steps below to upgrade firmware locally or remotely through VAP Access Point’s Web:

- Click “**Browse**” to select the firmware file you would like to load;
- Click “**Upload**” to start the upload process;
- Wait a few minutes, the VAP Access Point will reboot after successful upgrade.

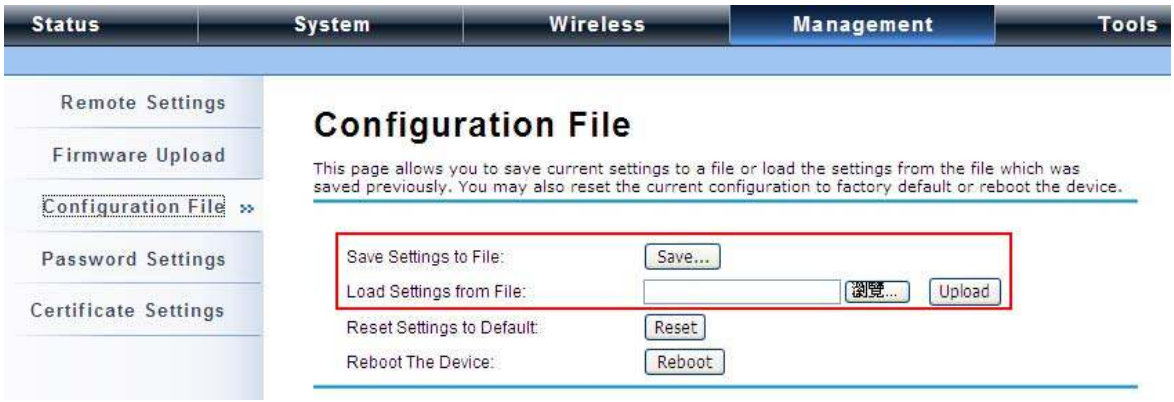
Note:

- Do NOT cut the power off during upgrade, otherwise the system may crash!

Backup/ Retrieve Settings

It is strongly recommended you back up configuration information in case of something unexpected. If tragedy hits your device, you may have an access to restore the important files by the backup. All these can be done by the local or remote computer.

Open "**Configuration File**" in "**Management**" as below:



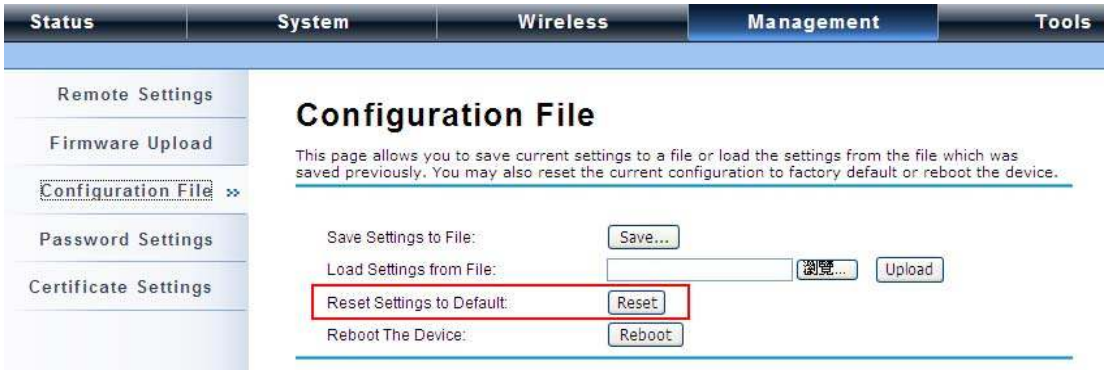
- **Save Setting to File**
  By clicking "**Save**", a dialog box will pop up. Save it, then the configuration file **ap.cfg** will be generated and saved to your local computer.

- **Load Settings from File**
  By clicking "**Browse**", a file selection menu will appear, select the file you want to load, like **ap.cfg**; Click "**Upload**" to load the file. After automatically rebooting, new settings are applied.

Restore Factory Default Settings

The VAP Access Point provides two ways to restore the factory default settings:

- **Restore factory default settings via Web**
  From "**Configuration File**", clicking "**Reset**" will eliminate all current settings and reboot your device, then default settings are applied.



- **Restore factory default settings via Reset Button**
  If software in VAP Access Point is unexpectedly crashed and no longer reset the unit via Web, you may do hardware reset via the reset button. Press and hold the button for at least 5 seconds and then release it until the PWR LED gives a blink.

Reboot

You can reboot your VAP Access Point from "**Configuration File**" in "**Management**" as below:
Click "**Reboot**" and hit "**Yes**" upon the appeared prompt to start reboot process. This takes a few minutes.

Password

From "**Password Settings**" in "**Management**", you can change the password to manage your IEEE 802.11b/g/n VAP Access Point.

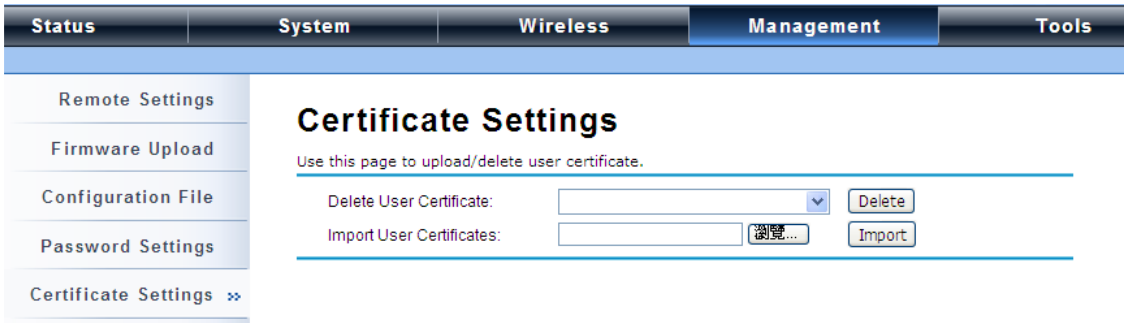
- **Current Password**: Enter the current password.
- **New Password:** Enter the new password.
- **Confirm Password:** Enter the new password again for confirmation.

Note:

- The password is case-sensitive and its length cannot exceed 19 characters!

Certificate Settings

Under Wireless Client mode, when EAP-TLS is used, the RADIUS server must know which user certificates to trust. The Server can trust all certificates issued by a given CA.
To import a user certificate, from Import User Certificates, click "**Browse**" and specify the location where the user certificate is placed. Click "**Import**".



- **Delete User Certificate:** Delete the selected user certificate.
- **Import User Certificates:** Imported the user certificate

4.3.5. Tools

System Log

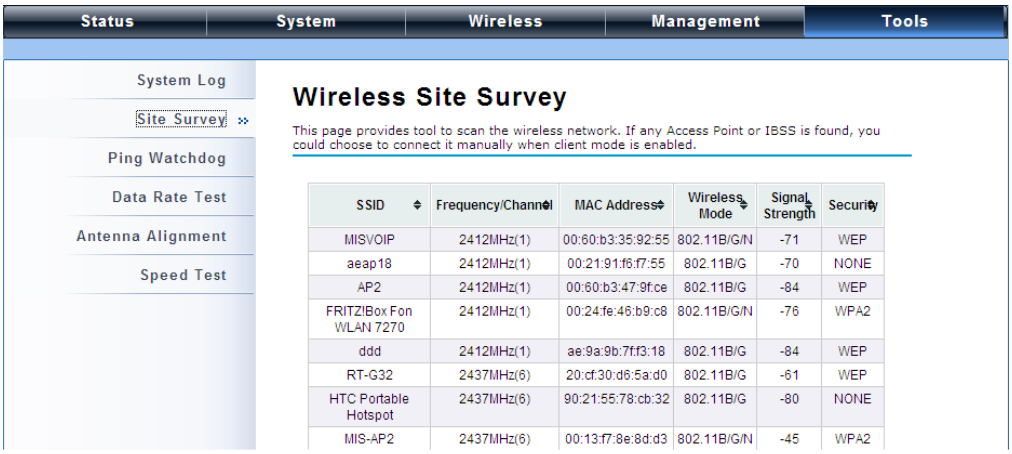
System log is used for recording events occurred on the VAP Access Point, including station connection, disconnection, system reboot and etc.

Open "**System Log**" in "**Tools**" as below.

- **Remote Syslog Server**
  Enable Remote Syslog: Enable System log to alert remote server.
  IP Address: Specify the IP address of the remote server.
  Port: Specify the port number of the remote server.

Site Survey

Only available under Wireless Client mode, site survey allows you to scan all the APs within coverage. Open "**Site Survey**" in "**Tools**" as below and select the desired AP to connect.


Status
System
Wireless
Management
Tools
System Log
Site Survey
Ping Watchdog
Data Rate Test
Antenna Alignment
Speed Test
Wireless Site Survey
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.
SSID Frequency/Channel MAC Address Wireless Mode Signal Strength Security
MISVOIP 2412MHz(1) 00:60:b3:35:92:55 802.11B/G/N -71 WEP
aeap18 2412MHz(1) 00:21:91:f6:f7:55 802.11B/G -70 NONE
AP2 2412MHz(1) 00:60:b3:47:9f:ce 802.11B/G -84 WEP
FRITZ!Box Fon WLAN 7270 2412MHz(1) 00:24:fe:46:b9:c8 802.11B/G/N -76 WPA2
ddd 2412MHz(1) ae:9a:9b:7f:f3:18 802.11B/G -84 WEP
RT-G32 2437MHz(6) 20:cf:30:d6:5a:d0 802.11B/G -61 WEP
HTC Portable Hotspot 2437MHz(6) 90:21:55:78:cb:32 802.11B/G -80 NONE
MIS-AP2 2437MHz(6) 00:13:f7:8e:8d:d3 802.11B/G/N -45 WPA2

Ping Watch Dog

If you mess your connection up and cut off your ability the log in to the unit, the ping watchdog has a chance to reboot due to loss of connectivity.

- **Ping Watchdog**
  Enable Ping Watchdog: To activate ping watchdog, check this checkbox.

  IP Address to Ping: Specify the IP address of the remote unit to ping.

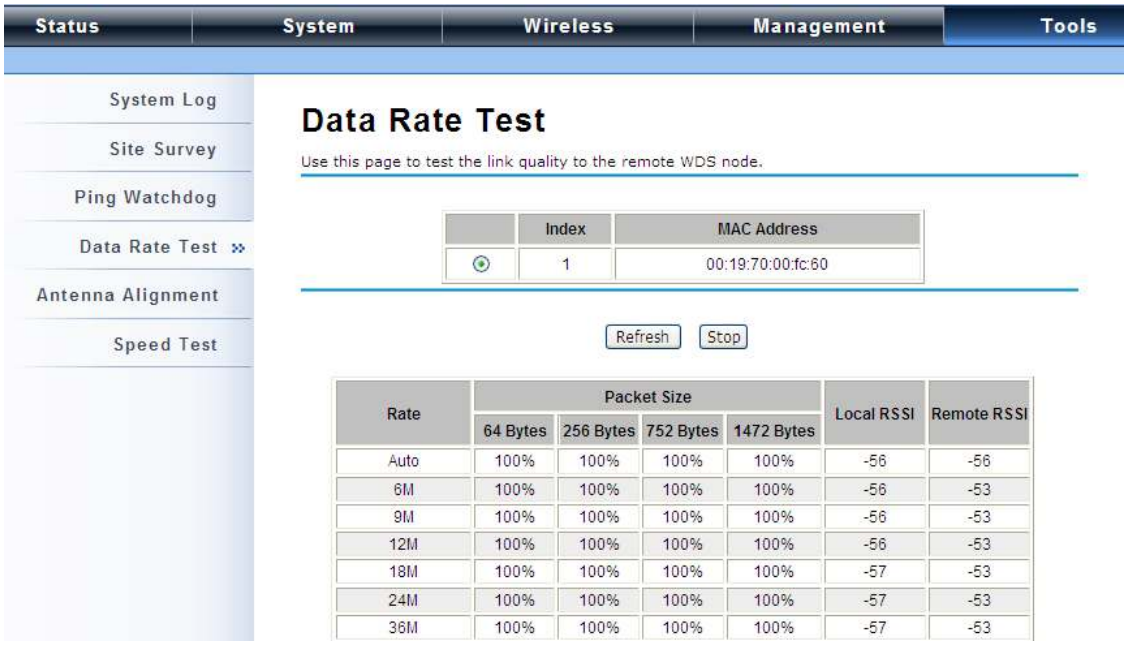
  Ping Interval: Specify the interval time to ping the remote unit.

  Startup Delay: Specify the startup delay time to prevent reboot before the VAP Access Point is fully initialized.

  Failure Count To Reboot: If the ping timeout packets reached the value, the IEEE 802.11b/g/n VAP Access Point will reboot automatically.

Date Rate Test

The Data Rate Test allows you to test the current RSSI at each data rate between your VAP Access Points.

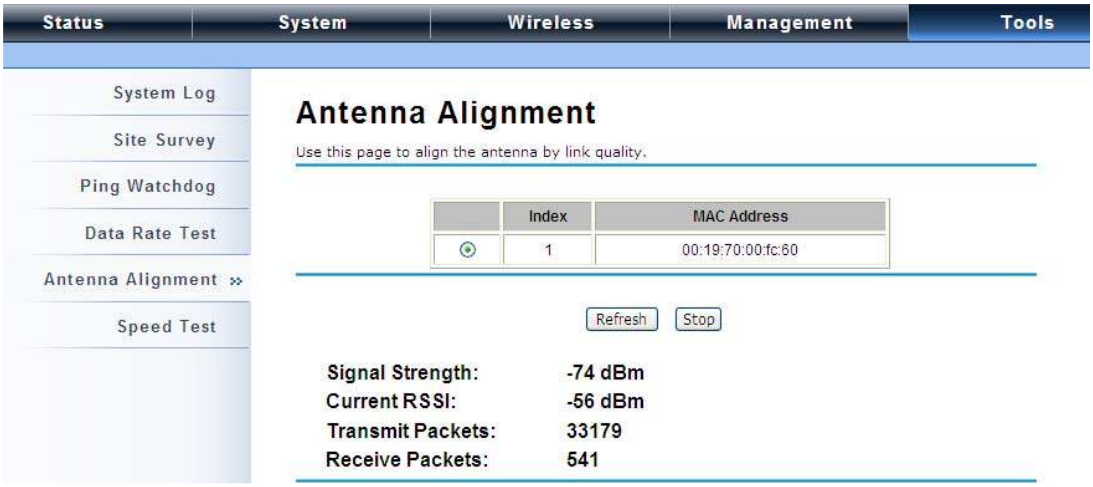


Antenna Alignment

Under Bridge mode, when the bridges are not easily visible from the location where the dish will be installed, the antenna alignment tool can help you evaluate the position of the unit and adjust the angle of the antenna more precisely. Keep it that in real circumstances a lot of additional factors should be taken into account when your unit is installed. These factors include various obstacles (buildings,

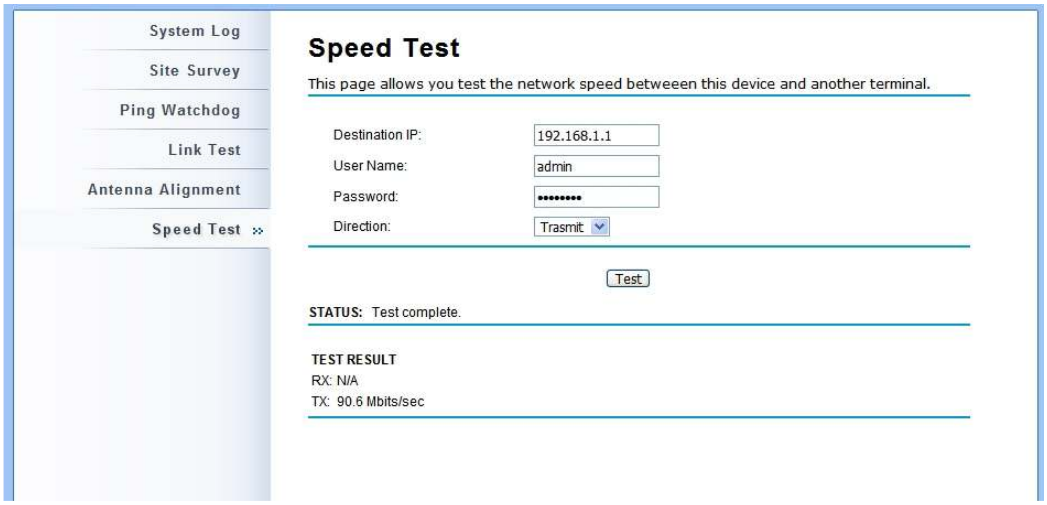
trees), the landscape, the altitude, transponder orientation, polarization, etc.

To use the tool, select the desired remote WDS bridge and click "**Start**", the web page will display the measured signal strength, RSSI and transmit/receive packets. If the signal quality is not quite good, try to adjust the antenna and see if the quality improves or not.



Speed Test

The speed test is to monitor the current data transmission (TX) and data reception (RX) rate with the remote 802.11an VAP Access Point. Enter the IP address of the remote CPE, type in the user name/password and click "**Test**". The result will display in the bottom **STATUS**. You may test single TX/RX or bi-direction.



5. Appendix A. ASCII

WEP can be configured with a 64-bit, 128-bit or 152-bit Shared Key (hexadecimal number or ACSII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ACSII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.

Table 1 ACSII

ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent	ASCII Character	Hex Equivalent
!	21	9	39	Q	51	i	69
"	22	:	3A	R	52	j	6A
#	23	;	3B	S	53	k	6B
$	24	<	3C	T	54	l	6C
%	25	=	3D	U	55	m	6D
&	26	>	3E	V	56	n	6E
‘	27	?	3F	W	57	o	6F
(	28	@	40	X	58	p	70
)	29	A	41	Y	59	q	71
*	2A	B	42	Z	5A	r	72
+	2B	C	43	[	5B	s	73
,	2C	D	44	\	5C	t	74
-	2D	E	45	]	5D	u	75
.	2E	F	46	^	5E	v	76
/	2F	G	47	_	5F	w	77
0	30	H	48	`	60	x	78
1	31	I	49	a	61	y	79
2	32	J	4A	b	62	z	7A
3	33	K	4B	c	63	{	7B
4	34	L	4C	d	64	|	7C
5	35	M	4D	e	65	}	7D
6	36	N	4E	f	66	~	7E
7	37	O	4F	g	67		
8	38	P	50	h	68		

6. Appendix B. SSH Settings

Table 2 CLI Commands

get	set	del	Keyword				Descriptions
√	√		system				--system setting
√				-swversion			--system firmware version
√	√			-systemmac			--system MAC address
√	√			-devmode			--system device mode AC or AP
√	√			-devname			--system name
√	√			-country			--country/region
	√			-ethernet1DataRate			--ether port 1 data rate
√	√			-ethernet2DataRate			--ether port 2 data rate
√	√			-macclone			--mac clone enable
√	√			-clonedmac			--cloned mac address
√	√			-poepower			--secondary RJ45 power
√	√			-stp			--Spanning Tree
√	√			-stpForwardDelay			--STP forward delay
√	√			-gpslatitude			--gps latitude
√	√			-gpslongitude			--gps longitude
√	√		ipset				
√	√			-networkmode			--network mode select (bridge or router)
√	√			-bridge			--bridge mode ip settings
√	√				-iptype		--fixed/dynamical ip(dhcp client)
√	√				-ipaddr		--ip address
√	√				-netmask		--subnet mask
√	√				-gateway		--gateway ip address
√	√				-dns1		--dns1
√	√				-dns2		--dns2
√	√			-router			--router mode ip settings
√	√				-wan		--wan ip settings
√	√					-accesstype	--router mode access type
√	√					-staticipaddr	--static ip address
√	√					-staticnetmask	--static subnet mask
√	√					-staticgateway	--static gateway ip address
√	√					-staticdns1	--static dns1
√	√					-staticdns2	--static dns2
√	√					-dhcpclienthost	--dhcp client hostname

						name	
√						-pppoeconnectstatus	--pppoe connect status
√						-pppoelocalip	--obtains IP from pppoe server
√	√					-pppoestaticipaddr	--pppoe static ip address
√	√					-pppoeusername	--pppoe username
√	√					-pppoepassword	--pppoe password
√	√					-pppoeservername	--pppoe server name
√	√					-pppoeconnectmode	--pppoe connect mode
√	√					-pppoeidletime	--pppoe idle time
√	√				-lan		--lan ip settings
√	√					-ipaddr	--lan ip address
√	√					-netmask	--lan subnet mask
√	√					-dhcpserverenable	--dhcp server enable
√	√					-dhcpserveripstart	--dhcp server ip start
√	√					-dhcpserveripend	--dhcp server ip end
√	√					-dhcpserverleasetime	--dhcp server leasetime
√	√					-dhcprelayenable	--dhcp relay enable
√	√					-dhcpserverip	--dhcp server ip
√	√		wlan				--wlan setting
√	√			-operationmode			--operation mode
√	√			-ssid			--wireless network name
√	√			-radio			--radio switch
√	√			-wirelessmode			--wireless mode
√	√			-lockApMac			--Lock to AP MAC
√	√			-HTprotect			--HT protect
√	√			-frequency/channel			-wireless frequency/channel (depends on country and wireless mode)
√	√			-power			--power
√	√			-rate			--rate
√	√			-antenna			--antenna type

√	√			-antennaGain			--antenna gain setings
√	√			-spaceInMeter			--wireless bwa space in meter setting
√	√			-LinkIntegration			--wireless bwa coverage class setting
√	√			-channelMode			--channel mode
√	√			-channelOffset			--channel offset of 40MHz
√	√			-extension			--extension
√	√			-A-MPDU			--A-MPDU
√	√			-A-MSDU			--A-MSDU
√	√			-shortGI			--short GI
√	√			-RIFS			--rifs
√	√			-RTS			--RTS
√	√			-fragment			--fragment
√	√			-beacon			--beacon
√	√			-DTIM			--DTIM
√	√			-preamble			--preamble
√	√			-IGMP			--IGMP
√	√			-stdm			--stdm setting
√	√			-cpeType			--CPE type
√	√	√		-key			--wireless wep key setting
√	√				-type		--wireless wep key type
√	√				-default		--wireless wep default key index
√	√	√			-1		--wireless wep key 1
√	√	√			-2		--wireless wep key 2
√	√	√			-3		--wireless wep key 3
√	√	√			-4		--wireless wep key 4
√	√	√		-eap			--WPA EAP setting
√	√	√			-eaptype		--WPA EAP Type
√	√	√			-innereaptype		--WPA inner EAP Type
√	√				-username		--WPA user name
√	√				-loginname		--WPA login name
√	√				-password		--WPA password
√	√				-usercert		--WPA cert file
√	√				-privatekeypassword		--WPA private key password
√	√			-trafficshaping			--traffic shaping

√	√				-enable		--enable Traffic Shaping
√	√				-downlimit		--Incoming Traffic Limit
√	√				-downburst		--Incoming Traffic Burst
√	√				-uplimit		--Outgoing Traffic Limit
√	√				-upburst		--Outgoing Traffic Burst
√	√			-wdsMac			--WDS Remote Mac
√					-local		--local macAddr
√	√				-remote1		--remote macAddr1
√	√				-remote2		--remote macAddr2
√	√				-remote3		--remote macAddr3
√	√				-remote4		--remote macAddr4
√	√			-wdsSeparation			--WDS Separation
√	√		vapprofile1(2, 3,etc)				--VAP setting
√	√			-active			--on/off this vap
√	√			-profileName			--Name of profile
√	√			-ssid			--ssid of this vap
√	√			-ssidhided			--Broadcast SSID Enable or Disable
√	√			-vlanID			--vlanID of this vap
√	√			-Isolation			--wireless separation
√	√			-wmm			--WMM Support
√	√			-MaxStaNum			--Max Station Number
√	√			-StaNumLmt			--Whether manually limit the number o f station
√	√			-bwenable			--Whether enable the VAP Traffic Shaping
√	√			-bwupstream			--VAP outgoing traffic limit stream
√	√			-bwupburst			--VAP outgoing traffic limit burst
√	√			-authentication			--wireless authentication type
√	√			-encryption			--wireless data encryption
√	√			-default			--wireless wep default key index
√	√			-wpa			--wireless WPA setting
√	√	√	√	-ac1			--access control
√	√				mode		--enable wireless access control (ACL)
	√	√			entry		--add or del ACL item

√		√			list		--delete or display all local ACL address
√	√			Portal			--captive portal
√				Association			--list of associated wireless clients
√				Statistics			--wireless status
√	√		vlan				--vlan setting
√	√			-active			--enable 802.1Q VLAN
√	√			-manageID			--Management VLAN ID
√	√		radius				--radius setting
√	√			-IPaddr			--IP address
√	√			-port			--port
	√			-shared secret			--Shared Secret
√	√			-key update			
√	√		firewall				--firewall setting
√	√			-srcipfilter			--source ip filter settings
√	√				-enable		--source ip filter enable
√	√				-addrule		--add a source ip filter rule
	√				-delerule		--delete source ip filter rule
√					-rulelist		--show source ip filter rule lists
√	√			-destipfilter			--destination ip filter settings
√	√				-enable		--destination ip filter enable
√	√				-addrule		--add a destination ip filter rule
	√				-delerule		--delete destination ip filter rule
√					-rulelist		--show destination ip filter rule lists
√	√			-srcportfilter			--source port filter settings
√	√				-enable		--source port filter enable
√	√				-addrule		--add a source port filter rule
	√				-delerule		--delete source port filter rule
√					-rulelist		--show source port filter rule lists
√	√			-destportfilter			--destination port filter settings
√	√				-enable		--destination port filter enable
√	√				-addrule		--add a destination port filter rule

	√				-delerule		--delete destination port filter rule
√					-rulelist		--show destination port filter rule lists
√	√			-portforward			--port forward settings
√	√				-enable		--port forward enable
√	√				-addrule		--add a port forward rule
	√				-delerule		--delete port forward rule
√					-rulelist		--show port forward rule lists
√	√			-udpptenable			--udp pass through enable
√	√			-dmzenable			--dmz enable
√	√			-dmzipaddr			--dmz ip address
√	√		remote				--remote management setting
√	√			-privacy			--radius IP address
√	√			-telnet			--enable telnet
√	√			-snmp			--enable snmp
√	√			-ftp			--enable ftp
√	√			-ssh			--enable ssh
√	√			-forcehttps			--force https
√	√			-wise			--enable wise tools
√	√		snmp				--SNMP setting
√	√			-version			--Protocol Version
√	√			-port			--Server Port
√	√			-getCommunity			--SNMP Read Community
√	√			-setCommunity			--SNMP Write Community
√	√			-trapdestination			--Trap Destination
√	√			-trapcommunity			--Trap Community
√	√			-v3Admin			--v3Admin
√	√				-on		--Enable SNMPv3Admin
√	√				-name		--name
	√				-password		--password
√	√				-accessType		--access type
√	√				-authentication		--Authentication Protocol
√	√				-Privacy		--privacy protocol
√	√			-v3User			-v3User
√	√				-on		--Enable SNMPv3User
√	√				-name		--name
	√				-passwor		--password

					d		
√	√				-accessType		--access type
√	√				-authentication		--Authentication Protocol
√	√				-Privacy		--privacy protocol
√	√			Location			--SNMP location
√	√		time				--time setting
√				-now			--current system time
√	√			-SetTime			--current time settings:YYYY.MM.DD-hh:mm:ss
√	√			-zone			--time zone
√	√			-NTPUpdate			-- NTP Update
√	√			-servertype			--server type
√	√			-IP			-IP
√	√			-Manual IP			-Manual IP
√	√		syslog				--syslog
√	√			-client			--enable syslog client
√	√			-ipaddr			--syslog server IP address
√	√			-port			--syslog server port number
	√			-clear			--syslog clear
√	√		pingwdg				--ping watchdog
√	√			-enable			--enable
√	√			-interval			--interval
√	√			-startdelay			--startup delay
√	√			-failcount			--failure count
√	√			-ip			--ip address
√			statistics				--statistics
√				-Wireless			--Wireless LAN
√				-Ethernet			--Ethernet LAN
√		√	log list				--syslog list
	√		password				--system password
	√		reset				--restore factory
	√		reboot				--reboot system
	√		exit				--logout from CLI